

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平10-505175

(43) 公表日 平成10年(1998) 5月19日

(51) Int.Cl.⁶

G 0 6 T 7/00

識別記号

F I

G 0 6 F 15/62

4 6 0

審査請求 未請求 予備審査請求 有 (全 76 頁)

(21) 出願番号 特願平8-508954
 (86) (22) 出願日 平成7年(1995) 8月29日
 (85) 翻訳文提出日 平成9年(1997) 2月28日
 (86) 国際出願番号 PCT/US95/11016
 (87) 国際公開番号 WO96/07156
 (87) 国際公開日 平成8年(1996) 3月7日
 (31) 優先権主張番号 08/298, 991
 (32) 優先日 1994年8月31日
 (33) 優先権主張国 米国 (US)

(71) 出願人 ベリフェラル ビジョン リミティド
 イギリス国, サマセット ビーエー11 3
 イージー, フロム, パリス ロード 57,
 パリス ハウス
 (72) 発明者 スミシーズ, クリストファー ポール ケ
 ネス
 イギリス国, ウィンボーン ビーエイチ21
 3ディーダブリュ, コルフェ ミュレ
 ン, パイン ロード 18
 (74) 代理人 弁理士 石田 敬 (外3名)

最終頁に続く

(54) 【発明の名称】 手書き署名を採取し、記憶し、伝送し、および、認証する方法ならびにそのシステム

(57) 【要約】

手書き署名を採取し確認するためのコンピュータベースの方法およびシステム。手書き署名は、電子的に記憶された文書といったような文書に関連する可能性がある。文書の画像が表示され、手書き署名が採取される(4)。手書き署名に関係する一揃いの計測値が決定され、署名エンベロープ(10)の中に記憶される。任意には、文書の検査合計値を決定し署名エンベロープ内に記憶することができる。署名者の請求されたアイデンティティも同様に署名エンベロープ内に記憶できる。署名エンベロープはコード化される(104)。署名エンベロープをもう1つのアプリケーションまたはコンピュータ・プラットフォーム(26)に通信することもできるし、または後に確認を行なうために記憶することもできる。署名エンベロープは復号され、署名エンベロープ内に記憶された一揃いの計測値は、署名者(6)のアイデンティティを確認するべく手書き署名測定値の既知のセットに対して比較される。システムには、確認済み署名情報(12)を記憶する署名テンプレートのデータベースが含まれている。確認済みの一揃いの署名計測値は、類似性

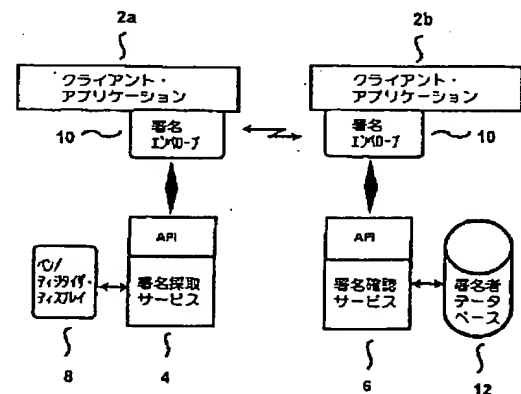


FIG. 2

【特許請求の範囲】

1. 電子文書に関連する手書き署名の電子表示を作成しその後手書き署名を確認するためのコンピュータベースの方法において、

第1のコンピュータ・プロセッサにおいて、文書の画像を電子的に表示する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって文書に署名する段階、

該第1のコンピュータ・プロセッサにおいて、前記手書き署名に関する一揃いの計測値を署名エンベロープの中に記憶する段階、

該第1のコンピュータ・プロセッサにおいて、文書の検査合計を作成する段階、

該第1のコンピュータ・プロセッサにおいて、前記署名エンベロープの中に検査合計を記憶する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の請求されたアイデンティティ（ID）を前記署名エンベロープの中に記憶する段階、

該第1のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化してコード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第2のコンピュータ・プロセッサへ伝送する段階、

該第2のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第2のコンピュータ・プロセッサにおいて、前記署名エンベロープ内に記憶された請求されたアイデンティティをもつ人物の手書き署名の確認済みの計測値セットを検索する段階、および

該第2のコンピュータ・プロセッサにおいて、確認済みの一揃いの計測値と前記署名エンベロープ内に記憶された一揃いの計測値とを比較して類似性評点を得る段階、

を含んで成るコンピュータベースの方法。

2. 前記のコード化された署名エンベロープをメモリ装置内に記憶する段階をさらに含んで成る請求の範囲第1項に記載の方法。
3. 前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第1項に記載の方法。
4. 前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第1項に記載の方法。
5. 前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第1項に記載の方法。
6. 前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第1項に記載の方法。
7. 前記第1のプロセッサにおいて、前記署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第1項に記載の方法。
8. 前記第1のプロセッサにおいて、前記署名エンベロープ内に前記第1のプロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第1項に記載の方法。
9. 前記第1のプロセッサにおいて、前記手書き署名の画像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲第1項に記載の方法。
10. 前記第1のコンピュータ・プロセッサに対して類似性評点を伝送する段階をさらに含んで成る請求の範囲第1項に記載の方法。
11. 第3のコンピュータ・プロセッサに対して類似性評点を伝送する段階をさらに含んで成る請求の範囲第1項に記載の方法。
12. 前記第2のプロセッサにおいて、前記電子文書の第2の検査合計を作成する段階、および
前記電子文書が前記第1のコンピュータ・プロセッサで署名された文書の真正な表示であるか否かを見極めるべく電気署名エンベロープ内に記憶された検査合計に対し第2の検査合計を比較する段階、
をさらに含んで成る請求の範囲第1項に記載の方法。

13. 電子文書のための手書き署名の電子表示を作成するためのコンピュータベースの方法において、

第1のコンピュータ・プロセッサにおいて、第1の文書の画像を電子的に表示する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって前記第1の文書に署名する段階、

該第1のコンピュータ・プロセッサにおいて、前記手書き署名に関する一揃いの計測値を前記署名エンベロープの中に記憶する段階、

該第1のコンピュータ・プロセッサにおいて、前記第1の文書の第1の検査合計を作成する段階、

該第1のコンピュータ・プロセッサにおいて前記署名エンベロープの中に前記第1の検査合計を記憶する段階、

該第1のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化してコード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第2のコンピュータ・プロセッサへ伝送する段階、

該第2のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第2のコンピュータ・プロセッサにおいて、第2の文書の第2の検査合計を作成する段階、および

該第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープ内に記憶された前記第1の検査合計に対して前記第2の検査合計を比較する段階、

を含んで成る方法。

14. 電子文書のための手書き署名の電子表示を作成するためのコンピュータベースの方法において、

第1のコンピュータ・プロセッサにおいて、第1の文書の画像を電子的に表示する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって第1の文書に署名する段階、

該第1のコンピュータ・プロセッサにおいて、前記手書き署名に関する一揃いの計測値を署名エンベロープの中に記憶する段階、

該第1のコンピュータ・プロセッサにおいて、第1の文書の検査合計を作成する段階、

該第1のコンピュータ・プロセッサにおいて署名署名エンベロープの中に第1の検査合計を記憶する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の指示を前記署名エンベロープの中に記憶する段階、

該第1のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化してコード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第2のコンピュータ・プロセッサへ伝送する段階、

該第2のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第2のコンピュータ・プロセッサにおいて、前記手書き署名が署名者のものであることを確認する段階、

該第2のコンピュータ・プロセッサにおいて、第2の文書の第2の検査合計を作成する段階、および

該第2のコンピュータ・プロセッサにおいて、前記第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内の第1の検査合計に対して前記第2の検査合計を比較する段階、
を含んで成る方法。

15. 1つの文書のための手書き署名の電子表示を作成するためのコンピュータベースの方法において、

第1の文書の画像を電子的に表示する段階、

署名者の手書き署名を電子的に採取することにより前記第1の文書に署名する

段階、

前記手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

前記第1の文書の第1の検査合計を作成する段階、

前記署名エンベロープ内に前記第1の検査合計を記憶する段階、

署名者の指示を前記署名エンベロープの中に記憶する段階、

該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープをメモリ内に記憶する段階、

該コード化された署名エンベロープを復号する段階、

前記手書き署名が署名者のものであることを確認する段階、

第2の文書の第2の検査合計を作成する段階、および

該第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープの中に記憶された第1の検査合計

に対して前記第2の検査合計を比較する段階、

を含んで成る方法。

16. 1つの文書に関連する手書き署名の電子表示を採取し、その後手書き署名を確認するためのコンピュータベースの方法において、

署名者の手書き署名を電子的に採取することにより文書に署名する段階、

該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階

文書の検査合計を作成する段階、

署名エンベロープ内に該検査合計を記憶する段階、

署名者の請求されたアイデンティティを前記署名エンベロープの中に記憶する段階、

該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープをメモリ内に記憶する段階、

該コード化された署名エンベロープを復号する段階、

前記署名エンベロープ内に記憶されたとおりの請求されたアイデンティティをもつ人物の、この人物の確認済み手書き署名に関する確認済みの一揃いの計測値を含む署名テンプレートを、メモリから検索する段階、および

前記署名テンプレート内に記憶された確認済みの一揃いの計測値と、前記署名エンベロープ内に記憶された一揃いの計測値とを比較して、文書に署名した時点で採取された手書き署名と前記確認済みの手書き署名との間の類似度を表す類似性評点を得る段階、
を含んで成る方法。

17. 電子文書の第2の検査合計を作成する段階、および

該電子文書が、署名された文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープ内に記憶された検査合計に対して第2の検査合計を比較する段階、

をさらに含んで成る、請求の範囲第16項に記載の方法。

18. 1つの文書のための手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

第1のコンピュータ・プロセッサにおいて、第1の文書の画像を電子的に表示する段階、

該第1のプロセッサにおいて、第1の文書を要約するプロンプトを電子的に表示する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって第1の文書に署名する段階、

該第1のコンピュータ・プロセッサにおいて、署名エンベロープの中に、前記手書き署名に関する一揃いの計測値を記憶する段階、

該第1のコンピュータ・プロセッサにおいて、署名者の指示を署名エンベロープ内に記憶する段階、

該第1のプロセッサにおいて、前記署名エンベロープ内にプロンプトを記憶する段階、

該第1のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第2のコンピュータ・プロセッサに伝送する段階、

該第2のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第2のコンピュータ・プロセッサにおいて、前記手書き署名が署名者のものであることを確認する段階、および

該第2のコンピュータ・プロセッサにおいて、前記署名エンベロープからプロンプトを検索する段階、
を含んで成る方法。

19. 前記プロンプトを表示する段階をさらに含んで成る、請求の範囲第18項に記載の方法。

20. 第1のコンピュータ・プロセッサにおいて、第1の文書の第1の検査合計を作成する段階、

該第1のコンピュータ・プロセッサにおいて、署名エンベロープ内に第1の検査合計を記憶する段階、

該第2のコンピュータ・プロセッサにおいて、第2の文書の第2の検査合計を作成する段階、および

該第2のコンピュータ・プロセッサにおいて、該第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内に記憶された第1の検査合計に対して前記第2の検査合計を比較する段階、
をさらに含んで成る、請求の範囲第18項に記載の方法。

21. 1つの文書のための手書き署名の電子表示を作成し確認するためのコンピュータベースの方法において、

第1の文書の画像を電子的に表示する段階、

該第1の文書の性質を識別する重要プロンプトを電子的に表示する段階、

署名者の手書き署名を電子的に採取することによって該第1の文書に署名する

段階、

該手書き署名に関連する一揃いの計測値を署名エンベロープの中に記憶する段階、

該署名エンベロープ内に、署名者の請求されたアイデンティティの指示を記憶する段階、

該署名エンベロープ内に重要プロンプトを記憶する段階、

該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

その後、該コード化された署名エンベロープを復号する段階、

前記手書き署名が署名者のものであることを確認する段階、および

署名者が前記第1の文書の性質についての情報提供を受けたことを確かめるため前記署名エンベロープから重要プロンプトを検索する段階、
を含んで成る方法。

22. 前記コンピュータベースの方法には、さらに、重要プロンプトを表示する段階が含まれている、請求の範囲第21項に記載の方法。

23. 前記手書き署名が署名者のものであることを確認する段階にはさらに、

前記署名エンベロープ内に記憶されているような署名者の請求されたアイデンティティをもつ人物の、この人物の確認済み署名の確認済み測定値を含む署名テンプレートを、メモリから検索する段階、

前記第1の文書の署名の時点で採取された手書き署名と確認された手書き署名の間の類似度を表す類似性評点を決定する段階、
が含まれている、請求の範囲第21項に記載の方法。

24. クライアント・アプリケーションの要請があった時点で、該クライアント・アプリケーションに対して類似性評点を伝送する段階をさらに含んで成る、請求の範囲第23項に記載の方法。

25. クライアント・アプリケーションに対して類似性評点を伝送す

る段階、および

該クライアント・アプリケーションに対して重要プロンプトを伝送する段階、
をさらに含んで成る請求の範囲第23項に記載の方法。

26. 前記第1の文書の第1の検査合計を作成する段階、

前記署名エンベロープ内に第1の検査合計を記憶する段階、

メモリ内に前記署名エンベロープを記憶する段階、

第2の文書の第2の検査合計を作成する段階、および

該第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープ内の第1の検査合計に対して前記第2の検査合計を比較する段階、

をさらに含んで成る請求の範囲第23項に記載の方法。

27. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、1つの文書のための手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

a. 第1の文書の画像を表示する段階、

b. 前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

c. 前記署名採取アプリケーションへと、第1の文書に関連するメッセージである重要プロンプトを移行させる段階、

前記署名採取アプリケーションの制御下で、

d. 署名採取ウィンドウを表示する段階、

e. 重要プロンプトを表示する段階、

f. ユーザーの手書き署名を電子的に採取することによって第1の文書にユーザーが署名できるようにする段階、

g. 該手書き署名に係する一揃いの計測値を署名エンベロープ内に記憶する段階、

h. ユーザーの請求されたアイデンティティの指示を該署名エンベロープ内に記憶する段階、

- i. 該署名エンベロープ内に前記重要プロンプトを記憶する段階、
 - j. 該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、
 - k. 前記クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、
 - 前記クライアント・アプリケーションの制御下で、
 - l. 前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および
 - 前記署名確認アプリケーション制御下で、
 - m. 前記のコード化された署名エンベロープを復号する段階、
 - n. 請求されたアイデンティティが署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテンプレートをデータベースから検索する段階、
 - o. 前記署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済みの一揃いの計測値と比較して類似性評点を得る段階、
 - p. 該署名エンベロープから前記重要プロンプトを検索する段階、および
 - q. 該重要プロンプトと類似性評点を前記クライアント・アプリケーションへと移行させる段階、
- を含んで成る方法。

28. 前記署名採取アプリケーションの制御下で、前記第1の文書の

第1の検査合計を作成し、前記署名エンベロープ内の第1の検査合計を記憶する段階、および

前記署名確認アプリケーションの制御下で、第2の文書の第2の検査合計を作成し、該第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内に記憶された第1の検査合計に対して前記第2の検査合計を比較する段階、

をさらに含んで成る請求の範囲第27項に記載の方法。

29. 前記署名採取アプリケーションが第1のコンピュータ・プロセッサ上で実行

され、前記署名確認アプリケーションが第2のコンピュータ・プロセッサ上で実行される、請求の範囲第27項に記載の方法。

30. 前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第27項に記載の方法。

31. 前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第27項に記載の方法。

32. 前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第27項に記載の方法。

33. 前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第27項に記載の方法。

34. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第27項に記載の方法。

35. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内にクライアント・アプリケーションを実行しているコンピュータ・プロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第27項に記載の方法。

36. 前記署名採取アプリケーションの制御下で、手書きの署名の画

像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲第27項に記載の方法。

37. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮されたビットマップ表示を前記署名エンベロープ内に記憶する段階をさらに含んで成る、請求の範囲第27項に記載の方法。

38. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

a. 前記署名採取アプリケーションが手書き署名を採取することを要請する段

階、

前記署名採取アプリケーションの制御下で

- b. ユーザーが手書き署名を電子的に入力できるようにする段階、
- c. ユーザーの手書き署名を電子的に採取する段階、
- d. 該手書き署名に関係する一揃いの計測値を算出する段階、
- e. 署名エンベロープ内に前記手書き署名に関係する一揃いの計測値を記憶する段階、
- f. ユーザーの請求されたアイデンティティの指示を前記署名エンベロープ内に記憶する段階、
- g. 前記署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、
- h. クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

- i. 前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

- j. 前記のコード化された署名エンベロープを復号する段階、
- k. 請求されたアイデンティティが前記署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテンプレートをデータベースから検索する段階、
- l. 該署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済み一揃いの計測値と比較して類似性評点を得る段階、
- m. 該類似性評点を前記クライアント・アプリケーションへと移行させる段階、

を含んで成る方法。

39. 前記クライアント・アプリケーションの制御下で、類似性評点を用いて、ユーザーがコンピュータシステム内の単数または複数のアプリケーションに対して

アクセスできるか否かを見極める段階をさらに含んで成る、請求の範囲第38項に記載の方法。

40. 前記クライアント・アプリケーションの制御下で、ユーザーがクレジットで商品を購入できるか否かを見極めるべく前記類似性評点を利用する段階をさらに含んで成る、請求の範囲第38項に記載の方法。

41. 前記署名採取アプリケーションが第1のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第2のコンピュータ・プロセッサ上で実行される請求の範囲第38項に記載の方法。

42. 前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第38項に記載の方法。

43. 前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第38項に記載の方法。

44. 前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第38項に記載の方法。

45. 前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第38項に記載の方法。

46. 前記署名採取アプリケーションの制御下で、署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第38項に記載の方法。

47. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に前記クライアント・アプリケーションを実行しているコンピュータ・プロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第38項に記載の方法。

48. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲第38項に記載の方法。

49. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮されたビットマップ表示を前記署名エンベロープ内に記憶する段階をさらに含んで成る、請求の範囲第38項に記載の方法。

50. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、1つの電子文書上の手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、前記クライアント・アプリケーションの制御下で、

- a. 文書の画像を表示する段階、
- b. 前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

段階、

前記署名採取アプリケーションの制御下で、

- c. ユーザーが手書き署名を電子的に入力できるようにする段階、
- d. ユーザーの手書き署名を電子的に採取する段階、
- e. 該手書き署名に関係する一揃いの計測値を算出する段階、
- f. 該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

段階、

g. ユーザーの請求されたアイデンティティの指示を該署名エンベロープ内に記憶する段階、

h. 文書の検査合計を作成する段階、

i. 前記署名エンベロープ内に検査合計を記憶する段階、

j. 該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

k. 前記クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

l. 前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

m. 前記のコード化された署名エンベロープを復号する段階、

n. 請求されたアイデンティティが前記署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテン

プレートデータベースから検索する段階、

o. 前記署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済み一揃いの計測値と比較して類似性評点を得る段階、および

p. 該類似性評点を前記クライアント・アプリケーションへと移行させる段階

を含んで成る方法。

51. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、1つの電子文書上の手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

a. 第1の文書の画像を表示する段階、

b. 前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

前記署名採取アプリケーションの制御下で、

c. ユーザーが手書き署名を電子的に入力できるようにする段階、

d. ユーザーの手書き署名を電子的に採取する段階、

e. 該手書き署名に関係する一揃いの計測値を計算する段階、

f. 該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

g. 第1の文書の第1の検査合計を作成する段階、

h. 前記署名エンベロープ内に検査合計を記憶する段階、

i. 該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

j. 前記クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

k. 前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

- l. 前記のコード化された署名エンベロープを復号する段階、
- m. 第2の文書の第2の検査合計を作成する段階、
- n. 前記第1の文書が該第2の文書と同じであるか否かを確認め

るべく前記第2の検査合計に対して前記署名エンベロープ内に記憶された第1の検査合計を比較する段階、および

- o. 前記第1の文書が前記第2の文書と同じであるか否かを前記クライアント・アプリケーションに情報提供する段階を含んで成る方法。

52. 前記署名採取アプリケーションが第1のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第2のコンピュータ・プロセッサ上で実行される、請求の範囲第51項に記載の方法。

53. 前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第51項に記載の方法。

54. 前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第51項に記載の方法。

55. 前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第51項に記載の方法。

56. 前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第55項に記載の方法。

57. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第51項に記載の方法。

58. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に前記クライアント・アプリケーションを実行しているコンピュータ・プロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第51項に記載の方法。

59. 署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲

第58項に記載の方法。

60. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮されたビットマップ表示を前記署名エンベロープ内で記憶する段階をさらに含んで成る、請求の範囲第51項に記載の方法。

61. 第1のクライアント・アプリケーション、第2のクライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記第1のクライアント・アプリケーションの制御下で、

a. 前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

前記署名採取アプリケーションの制御下で

b. ユーザーが手書き署名を電子的に入力できるようにする段階、

c. ユーザーの手書き署名を電子的に採取する段階、

d. 該手書き署名に関係する一揃いの計測値を計算する段階、

e. 該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

f. ユーザーの請求されたアイデンティティの指示を該署名エンベロープ内に記憶する段階、

g. 該署名エンベロープをコード化して、コード化された署名エンベロープを生成する段階、

h. 前記第1のクライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記第1のクライアント・アプリケーションの制御下で、

i. 前記のコード化された署名エンベロープを前記第2のクライアント・アプリケーションへと移行させる段階、

前記第2のクライアント・アプリケーションの制御下で

j. 前記のコード化された署名エンベロープを署名確認アプリケ

ーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

k. 前記のコード化された署名エンベロープを復号する段階、

l. 請求されたアイデンティティが前記署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテンプレートをデータベースから検索する段階、

m. 前記署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済み一揃いの計測値と比較して類似性評点を得る段階、および

n. 該類似性評点を前記第2のクライアント・アプリケーションへと移行させる段階、

を含んで成る方法。

62. 前記第2のクライアント・アプリケーションの制御下で、前記類似性評点を利用して、ユーザーがコンピュータシステム内の単数または複数のアプリケーションおよびデータにアクセスできるか否かを見極める段階をさらに含んで成る、請求の範囲第61項に記載の方法。

63. 前記第2のクライアント・アプリケーションの条件下で、ユーザーがクレジットで商品を購入できるか否かを見極めるべく前記類似性評点を利用する段階をさらに含んで成る、請求の範囲第61項に記載の方法。

64. 前記署名採取アプリケーションが第1のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第2のコンピュータ・プロセッサ上で実行される、請求の範囲第61項に記載の方法。

65. 前記第1のクライアント・アプリケーションが第1のコンピュ

ータ・プロセッサ上で実行され、前記第2のクライアント・アプリケーションが第2のコンピュータ・プロセッサで実行される、請求の範囲第61項に記載の方法。

66. 前記第1のコンピュータ・プロセッサが第1のオペレーティングシステムに従って動作し、前記第2のコンピュータ・プロセッサが第2のオペレーティングシステムに従って動作する、請求の範囲第65項に記載の方法。

67. 前記署名採取アプリケーションが第1のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第2のコンピュータ・プロセッサ上で実行される、請求の範囲第65項に記載の方法。

68. 前記署名採取アプリケーションが第3のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第4のコンピュータ・プロセッサ上で実行される、請求の範囲第65項に記載の方法。

69. 電子文書のための手書き署名の電子表示を作成するためのコンピュータベースのシステムにおいて、

署名者の手書き署名を電子的に採取することにより、署名者が第1の文書に署名できるようにするための手段、

署名エンベロープ内に、該手書き署名に関係する一揃いの計測値を記憶するための手段、

前記第1の文書の第1の検査合計を作成するための手段、

前記署名エンベロープ内に前記第1の検査合計を作成するための手段、

署名者の指示を前記署名エンベロープ内に記憶するための手段、および

該署名エンベロープをコード化して、コード化された署名エンベ

ロープを作成するための手段、

を含んで成るシステム。

70. 前記のコード化された署名エンベロープを復号するための手段、

該署名エンベロープ内に記憶されている手書き署名が署名者のものであることを確認するための手段、

第2の文書の第2の検査合計を作成するための手段；および

該第2の文書が前記第1の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内に記憶された第1の検査合計に対して前記第2の検査合計を比較するための手段、

をさらに含んで成る、請求の範囲第69項に記載のシステム。

71. 前記のコード化された署名エンベロープをメモリ内に記憶するための手段をさらに含んで成る、請求の範囲第70項に記載のシステム。

72. 第1のプロセッサに手書き署名を電子的に入力するための手段、

署名者の手書き署名を電子的に採取するための手段、

署名エンベロープ内に該手書き署名に関係する一揃いの計測値を記憶するための手段、

署名者の請求されたアイデンティティを入力するための手段、

前記署名エンベロープ内に署名者の請求されたアイデンティティを記憶するための手段、

前記署名エンベロープをコード化して、コード化された署名エンベロープを作成する手段、および

該コード化された署名エンベロープを遠隔の署名確認センターに通信するための手段、

を含む、前記手書き署名を採取するための複数の第1のプロセッサ、および

前記第1のプロセッサの1つからコード化された署名エンベロープを受理するための手段、

該コード化された署名エンベロープを復号するための手段、

確認済みの一揃いの署名計測値を含み署名者の請求されたアイデンティティに対応する署名テンプレートを検索するべくデータベースをアクセスするための手段、

前記確認済みの一揃いの署名計測値と、前記署名エンベロープ内に記憶された一揃いの計測値とを比較することによって前記手書き署名を確認するための手段、

前記署名エンベロープ内に記憶された一揃いの計測値と前記確認済みの一揃いの署名計測値との間の類似性を表す類似性評点を決定するための手段、

前記第1のプロセッサの1つに対して該類似性評点を通信するための手段を含み前記署名テンプレートのデータベースに結合された第2のプロセッサによって制御され、複数の第1のプロセッサの各々との関係において遠隔に位置づけられているもののそれに対し電子的に結合されている署名確認センター、を含んで成る、署名確認センターシステム。

73. 第1のプロセッサに手書き署名を電子的に入力するための手段、
署名者の手書き署名を電子的に採取するための手段、
署名エンベロープ内に該手書き署名に関係する一揃いの計測値を記憶するための手段、
署名者の請求されたアイデンティティを入力するための手段、
前記署名エンベロープ内に署名者の請求されたアイデンティティを記憶するための手段、
該署名エンベロープをコード化して、コード化された署名エンベ
ロープを作成する手段、および
該コード化された署名エンベロープを遠隔の署名確認センターに通信するための手段、
を含む、手書き署名を採取するための複数の第1のプロセッサ、
署名者についての確認済みの一揃いの署名計測値を含み各々の署名者のアイデンティティにより指標付けされた複数の署名テンプレートを含む確認済みの手書き署名データを記憶するための中央データベース、
前記第1のプロセッサの1つからコード化された署名エンベロープを受理するための手段、
該コード化された署名エンベロープを復号するための手段、
署名者の請求されたアイデンティティに対応する署名テンプレートを検索するべく前記中央データベースをアクセスするための手段、
前記確認済みの一揃いの署名計測値と、前記署名エンベロープ内に記憶された一揃いの計測値とを比較することによって前記手書き署名を確認するための手段、
前記署名エンベロープ内に記憶された一揃いの計測値と前記確認済みの一揃いの署名計測値との間の類似性を表す類似性評点を決定するための手段、
前記第1のプロセッサの1つに対して該類似性評点を通信するための手段を含み前記署名テンプレートの中央データベースに結合された第2のプロセッサによって制御され、前記複数の第1のプロセッサの各々との関係において遠隔に

位置づけられているもののそれに対し電子的に結合されている署名確認センター

、
を含んで成る、署名確認センターシステム。

【発明の詳細な説明】

手書き署名を採取し、記憶し、伝送し、および、認証する方法ならびにそのシステム

発明の分野

本発明は手書き署名を電子方式で記憶保存する方法およびシステムに関し、より詳しくは、電子方式で記憶した手書き署名、および、それに関連する文書の確認を複数のプラットフォーム（Platform）で実施可能にする方法およびシステムに関するものである。

著作権に関する注意

ここに開示する特許書類の一部には、著作権による保護の対象となる事項が含まれている。したがって、著作権者は、上記特許書類またはその開示事項が特許庁の管掌する特許ファイルまたは記録に現われた際には、何人による複写再生にも対抗するものではないが、それ以外の場合には何事によらず、この著作権に関する全ての権利を保持するものである。

発明の背景

机上設置型にしる携帯型にしる、電子ペンまたはディジタイザによるデータ入力を可能にした多くのコンピュータシステムが設計されている。手書きの字句を認識し、標準テキストに翻訳するソフトウェアも世に出ている。また、電子ペン入力を利用したアプリケーションも数多く存在している。ペン入力は、コンピュータキーボードに馴染みのない人や苦手な人にもコンピュータを楽に使用できるようにしている。さらに、ペン入力型コンピュータの使用、ディジ

タル形式による情報の記憶、およびその伝送は、紙の使用を減らしまたはそれを廃止するといったような重要な商業上の利益を実現している。

ディジタイザは、典型的に、ペン先の位置を1秒間に約100回サンプルし、そして一インチの70分の一の動きを感知する感度を有している。したがって、ディジタイザは人間の手の動きを極めて正確に記録することができる。コンピュータによる署名確認はこの点を利用して目に見える署名の形だけではなく、署名の速さおよび書くりズム等の署名の動的な面を分析することができる。

ペン入力（例えば、手書き署名）を取り込み、ペン入力の基本的な特徴を決定し、そしてそのペン入力を電子方式で表すことを可能にするアルゴリズムがある。また、電子方式の手書き署名が同一人のものか否かを決定することができるアルゴリズムもある。これらは、例えば米国特許第5,109,426号（英国特許出願第90 24393.3号）、米国特許第4,495,644号、および英国特許出願第1480066号等に開示されているが、ここでの詳細な説明は省略する。

署名の確認は、コンピュータの安全性に対し非常に重要な貢献をすることができる。コンピュータの他の全ての安全機構は、個人のみが知る事項（例えば、パスワード）、または所有する物（例えば、物理的なキー）に依存している。署名の確認は、このようなものに頼る代わりに、盗難または漏洩の心配のない身体の動作の様子に依存することによって、コンピュータ使用者の真の同一性に関する確実な証拠を提供する。

現在まで署名の確認は、主としてアクセス領域の安全性の観点から、コンピュータシステムの全てまたは一部に対する使用者のアクセスを許す前に、本人であることを確認する目的で採用されてきた。

しかし、紙に書く伝統的な署名は、契約書あるいは遺言書に署名

するとか、為替を切る際には支払い拒否に対抗するための保護手段として署名するといったように、種々の意志または意図を証明するのに使用されている。

コンピュータ化された書類の利用が可能になっているにも拘わらず、紙面への署名に対する法的、または文化的要求から、今日でもなお多くの分野で紙に依存することが必要である。

したがって、デジタル形式、即ち電子方式の文書よりも、それと同じハードコピーの方が好まれる場合がしばしば生じている。例えば、土地譲渡に関する遺言書とか契約書は、殆ど全ての司法管轄区域における法律によって、それが手書きであること、およびその書面に対する当事者並びに証人の手書き署名原本を含んでいることが要求される。文書が電子方式で作成されている場合、文書の内容を比較的簡単に改竄できるため、後日見る書面が最初に作成された物と同一であるかが不確かであることが多い。ペン入力機能を使用して取り込んだ手書き署名

は文書のテキストに組み入れることはできるが、後日見る文書が“電子的に”署名されたものであるかは、決して確かとはいえない。

したがって、手書き署名の採取 (Capture) および確認の科学を安全アクセス機構としてより、もっと広範な面に適用することが望ましいだろう。特に、ある意図 (例えば、法的文書に署名したことの意図) を証明する領域においては、署名された文書とその署名者の署名とを関連付ける確実な署名採取および確認方法が必要になる。

現存のシステムは、電子方式による署名がその後改竄されたかどうか、そして電子文書に関連するその電子方式の署名がその文書の処理 (作成) 時点で採取されたどうかに焦点を当ててきた。例えば、キャップ (Kapp) 等に付与された米国特許第5,195,133号は、商業上の責務を認めるという趣旨の署名が問題処理 (文書作成) 時点で

行われ、そしてその署名が他の問題処理に関して採られた本物の署名ではなく、またその処理に関するデジタル記録に詐欺的に組み込まれたものではないことを保証する機構について述べている。このキャップ等によるシステムと同様なシステムは、処理に関するデジタル記録を作成し、その処理時点でなされた署名のデジタル表示を採取し、処理のデジタル記録を使用して署名のデジタル表示を記号化している。この方法は、署名の表示が、署名したといわれている時点で署名されたものであることを保証することをその目的としてる。しかし、このような手法はデジタル形式で採取した手書き署名が後で修正されたかどうかについては確認がとれない。さらに、キャップ等による手法に見られるようなシステムは処理 (文書作成) を必要とするから、処理を伴わない環境下で署名を採り、確認するという操作は不可能である。

現存の手書き署名の採取および確認システムは、単一のプラットフォームで使用するよう構成されている。手書きの署名を符号化して、他のアプリケーションが電子方式の手書き署名を利用できないようにすることがしばしば行われる。しかし、インターネットを含む今日の進歩したコンピュータ間通信のおかげで、多くのアプリケーションは、署名が行われたときと同じ機器または同じ時間に確

認をすることを要求しないだろう。例えば、手書き署名を一つの装置で電子的に採取し、記憶し、もう他のコンピュータ・プラットフォームに電子的に伝送し、その後で確認するシステムが望ましい。したがって、統合されたプラットフォーム間署名確認システムが必要になる。特に、特定の基礎となるハードウェアを前提とせず、かつ異種のコンピュータおよび異種のオペレーションシステム間で移動が可能なシステムが必要である。

多くの業務機関および政府機関の部局が、文書に署名を求めるこ

とはよくあることである。例えば、小切手またはクレジットカードで物を買うとき、レンタカーの契約をするとき、リース契約をするとき、運転者登録またはその他の政府許可を申請するとき、選挙の日、または試験の受験証明等々である。また、署名を求める人が、署名を求められた個人を熟知せず、要請に基づいてした署名を対比照合するその署名者の本物の署名を持ち合わせていない、といったことはよくあることである。さらに、照合のために本物の署名が用意されていたとしても、署名を要求する者が、二つの署名が同一人によるものかどうかの判定に未熟であったりすることもよくあることである。したがって、一つの場所で署名を採取し、それを多くの個人に関する確認済みの署名行動を記録している中央局に電氣的に伝送し、そして署名者の身元確認を署名地に返すシステムが必要である。

また、ある場合には、契約書またはその他の法的書類に署名した者が後日、署名した文書の性質を理解していなかったこと、または彼または彼女が文書に署名したときに誤解させられたことを主張して、彼または彼女の責務を終了させようとすることがある。さらに、マルチウインドウコンピュータ環境下では、電子的に文書に署名した者が、実際に署名したコンピュータのどの文書に記録されているかが不確かになるかもしれない。もし記録が署名時点でなされたとすれば（それは後から取り出せる）、文書に署名する際に署名人が何を告げられたかを記録し、署名する前に、これから署名する文書の正体、性質、および重要性に関して署名人に警告することが有用である。

要するに、署名採取が必要とされる多様な環境において、手書き署名採取およ

び確認技術の応用を可能にすることによって、電子ペン入力装置の高まりつつある利用性を用いるシステムが必要である。

発明の要約

したがって、本発明は手書き署名を電子的に採取し、この署名を電子方式で記憶し、採取した手書き署名を伝送し、そして採取した手書き署名を認証するための方法およびそのシステムを提供するものである。

本願において使用する“署名”という表現は、その意志または同意を表す者によってなされた手書きの標し（マーク）を意味するものとする。そして、この言葉は通常その者の自署と考えられるものを含んでいる。また、“署名した、または署名された”という表現は、署名に対応する意味を有し、その書き物を認証する意図を持つ当事者によって書かれ、または採用された如何なる記号も含むものとする。その場合、その書き物は電子方式によるのものであってもよい。ただし、本願において使用する“署名”は、以下のものを含まないことに注意されたい。即ち、“デジタル署名”としてコンピュータ科学の分野で知られるようになったもの、言い換えれば、電子文書を作成し、または伝送する本人を確定する電子コードを含まない。“デジタル署名”は、手書き署名を、特定の個人に与えられかつ秘密に保持しなければならない暗唱英文字数字“キー”でもって置き換える機能を有している。これとは対照的に、本発明は人の手書き署名を電子的に採取し、かつ、処理することを指向するものである。

本発明の代表的な実施例では、公知の電子ペンベースのハードウェアを利用して、手書き署名を電子的に採取している。

本発明の代表的な実施例は、署名採取モジュール、署名確認モジュール、およびテンプレート（Template）・データベースを含んでいる。

署名採取モジュールは本人の署名を採取し、その署名行為を示す（または記録する）署名エンベロープ（署名包袋）を作る。署名エンベロープは電子方式、例えば電子ペンベースのコンピュータスクリーン上で採取された署名の手書きに関連する一定のデータを記録する。典型的には、署名採取モジュールはクライアント

ト・アプリケーションによって呼び出され、制御され、そしてこれと通信を行う。

例えば、クライアント・アプリケーションは文書に関する手書き署名を要求することができる。クライアント・アプリケーションが署名採取モジュールを呼び出すと、このモジュールはコンピュータスクリーン上に署名採取用ウィンドウを表示して、クライアントに対し当該コンピュータスクリーン上の署名採取用ウィンドウに彼または彼女の署名（例えば、電子鉄筆を使用して）を書くことを要求する。これに対して、クライアント・アプリケーションは署名採取モジュールに対して、署名した文書の識別記号、そして／または文書に署名した理由（または文書の重要性）を送る。重要プロンプト（グラビティ・プロンプト：Gravity Prompt）と称するこの情報は、使用者に対し署名採取モジュールによって署名採取ウィンドウに示される。この表示によって使用者は、署名されている文書が彼または彼女が署名したと思う文書を確認でき、さらに使用者に署名行為の理由およびその重要さを警告する。

使用者が文書に署名するとき（例えば、ペンまたは鉄筆をスクリーン上に走らせて）、鉄筆の移動軌跡を描く画像（イメージ）が現れる。したがって、使用者の署名（即ち、自署）が使用者に対して表示される。署名時、署名採取モジュールは署名行為に関してある一定の特色、例えば署名の大きさ、曲線の形状と相対的位置、ループ、直線、点、斜線、その他書いた署名の特色と共に、署名に特色を与える相対速度等を測定する。これらの測定は“署名行為統計”

（Act-of-signing Statistics）”と呼ぶことができる。

本発明による代表的実施例では、署名採取モジュールは署名された文書の検査合計値（Checksum）を作成する。この文書の検査合計値は、署名した申立てを受けている文書が、確かに署名されたこと、さらにこの文書に何ら変更が加えられていなかったことを後日確認するのに使用することができる。

代表的な実施例では、文書の検査合計値は文書原本の完全な陳述書を構成するものではなく、同原本をこの文書の検査合計値から起こすことはできない。文書の検査合計値は文書に対して数学的関係を持っている。もし文書が変更されると

、文書はもはや検査合計値に対して数学的整合性を維持することができなくなる。

上記実施例に代わる実施例では、文書の検査合計値に加えて、あるいはそれに代わるものとして、署名された文書の圧縮表示を作成することが可能である。

署名採取モジュールはデータ、中でも署名行為統計、署名の日時、署名人請求の識別記号、重要プロンプトに現れる言葉、文書検査合計値、そして選択的には、署名の図形画像を示すデータをコード化する。そして、この署名採取モジュールはこれらコード化データを含む署名エンベロープを作成する。代表的実施例では、署名エンベロープはコード化文字列データとなる。したがって、この署名エンベロープは書込み時点における諸事項を示すための確実な方法である。

また、代表的な実施例によれば、クライアント・アプリケーションが署名エンベロープに含まれている情報を解読したりまたは変更したりすることはできない。

署名確認モジュールは、特定の署名が本物である確率を報告する。署名確認モジュールはテンプレート・データベースにアクセスする

ことができる。このテンプレート・データベースは複数のテンプレートを記憶している。各テンプレートは個人の署名行為統計と、その個人に関する既知の識別記号とを含んでいる。各テンプレートは、制御された登録処理過程を介して作成され、そして後日のアクセス用としてテンプレート・データベースに記憶される。

代表的な実施例では、署名確認モジュールおよびテンプレート・データベースは、多くのクライアント・アプリケーションからアクセスできる離れた位置にある。例えば、署名確認モジュールとテンプレート・データベースは、独立した中央署名確認局に設けられる。これに代わる他の実施例では、上記の署名確認モジュールとテンプレート・データベースは、必要に応じてクライアント・アプリケーションからアクセスできる局部システムに設けられる。

クライアント・アプリケーションが署名確認をするとき、クライアント・アプリケーションは確認対象署名の署名エンベロープを署名確認モジュールに送る。

各クライアント・アプリケーションは、そのクライアント・アプリケーションによって作成された署名、またはその他のクライアント・アプリケーションによって以前に作成した署名を確認することができる。

例えば、署名採取モジュールを多くのコンピュータ、例えばペン書込みベースのポータブルコンピュータに内蔵させ、一つのホストコンピュータに署名確認モジュールを設けることもできる。ポータブルコンピュータはいつでも多くの署名を採取して（したがって、多くの署名エンベロップを作成し）、それを署名確認用のホストコンピュータに伝送する。

署名確認モジュールが特定の署名エンベロップを受けたときに、この署名確認モジュールは、上記の署名エンベロップが同署名エンベロップにて識別されている使用者による真の署名書き込み時に作

成されたものかどうかを評価するよう署名確認モジュールに指示することができる。署名確認モジュールは署名エンベロップを解読し、当該署名エンベロップに含まれている情報と、テンプレート・データベースに記憶されている署名テンプレートとを比較することができる。この比較に基づいて、署名確認モジュールは署名の整合性に関する百分率（例えば、78%）を決定し、この百分率および署名エンベロップに記憶されているその他の情報をクライアント・アプリケーションに報告する。

したがって、本発明は電子的に採取した手書き署名を、これまでの紙を用いた署名と同じように使用することを可能にするものである。本発明によって採取された署名は、偽造および詐欺行為の検出および防止を支援するコンピュータ技術によって、伝統的な紙に書く署名の持つ「性能」を凌ぐであろう。

本発明は、現存のソフトウェアプログラムと共に使用できるように設計されている。例えば他のコンピュータプログラムによって作動するソフトウェア要素として使用できるように設計されている。また、本発明は使用者のコンピュータネットワークへのアクセスを可能にする防護安全プログラムの一部として、ワードプロセッサの一部として、あるいは電子メールプログラム（Eメールプログラム）の一部として（例えば、Eメールメッセージ発信人の識別記号確認に）使

用することができる。本発明は特に署名の採取および確認に係る処理を行う。(ここで用いられているように、本発明によるモジュールを利用するプログラムを「クライアント・プログラム」という)。

したがって、クライアント・プログラムは本発明を用いてあらゆる目的のために署名を採取することができる。本発明は同意を示す伝統的なやり方(署名)を新たな技術環境に進展させると共に、紙

使用の必要性をなくすことできる。例えば、本発明による署名採取モジュールは、ディジタイザが取り付けられているケーブルテレビの変換ユニット(時には「セットトップボックス(set-top box)」と言われる)に内蔵させることができるから、視聴者は本発明を用いて種々の物品およびサービスの供給権限をその供給者に与えることができる。そこで採取された署名は供給者のシステムに伝送され、そこで物品、サービスの配送前に署名確認モジュールに送ることができ、事柄(取引:Event)の記録として保管される。この方法の利点は家族構成員めいめいが個人のカードを持ち歩いたり、それに“暗証番号”を付けたりすることをせずに、個人化(例えば、親、子供等)ができる点である。また、署名採取モジュールを例えば、裏面に適当なタッチセンサ式ディジタイザを取り付けた手持ち型の遠隔制御ユニットに設ければ、本発明の能力は容易に高められる。

もう一つの例は、車販売店で車を買うためにローンを組む場合である。手書き署名は署名採取モジュールによって採取することができる。この結果として生じた署名エンベロープは独立の署名確認局に送付される。この確認局から返されてきた確認記録を使って、車が買い手の手に渡る前に、全体のクレジット査定が計算される。

また、署名はそれに続く確認を要しない場合とか、ある個人がした署名がその受取人にとって初めてのものである場合にも採られる。例えば、新郎新婦による結婚許可宣誓書への署名、客によるホテル登録用紙への署名、および、小包配達書への署名等である。

したがって、署名は、例えば、遠隔地にあるコンピュータシステムにアクセスを許可する前にその確認のために遠隔地に送ることができる。また、署名は特定

の人が特定の文書または処理を許可したことの記録としてコンピュータのアーカイブ（保管所：Archive）

に記憶される。また、使用者に特定の電子文書へのアクセスを許可してよいかどうかを即座に決定するために署名を確認することが望ましい。

本発明は署名データ（特に署名エンベロープ）が詐欺的誤用を受けることを許さない。したがって、クライアント・プログラムは、コード化形式のものを除く署名データへのアクセスを行うことはできないし、また偽造に対し実質的に助けとなると思われる情報を得ることはできない。

本発明の独特な安全性は以下の点にある。即ち、本発明では、生の署名データを署名確認装置に伝送するのではなく（即ち、署名採取モジュールが生署名データを署名確認モジュールに伝送するのではなく）、署名採取の段階で署名の特色抽出が行われる。代表的な実施例では、生の署名データは署名エンベロープに記憶されず、また如何なる段階に置いてもクライアント・プログラムが利用できないようにしてある。したがって、署名エンベロープを調べて生の署名データを改造し、その後でその生の署名データをシステムに再度挿入することができないようにしてある。また、このことは署名確認前に伝送または保管される情報量を削減する。

本発明は電子文書の不法修正の検出補助に利用できる。上記したように、文書の検査合計値は文書を形成している文字コードから計算され、署名エンベロープの一部としてその文書とは別に記憶される。修正文書から得られる文書の検査合計値は元のものとは違うから、その修正を検出することができる。本発明は、インクが紙上で乾くことに対する完全な電子的比喩を支持して、進歩した検査合計方法を用いて署名エンベロープを文書に結びつける。このことは、重要プロンプトと共に、一文書に対してなされた署名が他の文書に使用されないように、一署名一意使用の維持を支援するものである。

図面の簡単な説明

図1は本発明による典型的なシステム構造を示すブロック図である。

図2は第1のプラットフォームで採取された署名を、第2のプラットフォームで確認する場合に使用するような本発明による典型的なシステム構造を示すブロック図である。

図3は手書き署名の採取に使用するウィンドウおよび重要プロンプトの例を示す図である。

図3Aは他の重要プロンプトの例を示す図である。

図4は署名エンベロープのライフサイクルを示す流れ図である。

図5は署名採取過程の典型的段階を示す流れ図である。

図6は本発明によるテンプレート・ソフトウェアオブジェクトに関する典型的なライフサイクルを示す流れ図である。

図7はテンプレート登録過程の典型的な段階を示す流れ図である。

図8は本発明のエンティティ (Entity) に関するエンティティ関係図である。

図9は人物を表すソフトウェアオブジェクトのライフサイクルを示す図である。

詳細な説明

図面参照にて、図1には本発明の構成要素を利用した典型的なシステムがブロック図形式で示されている。

第1図は署名の採取と確認の機能が同一装置で実行される構成を示すものである。クライアント・アプリケーション2は署名の採取を要求する。このクライアント・アプリケーションはこの要求情報

を署名採取モジュール4 (署名採取サービスとも呼ばれる) に提示し、そしてこの署名採取モジュールはユーザーが彼のまたは彼女の署名を適当なハードウェア装置、例えば、ペン/ディジタイザとディスプレイ6との組合せを使用して署名することを要求する。この署名採取モジュール4は、後述するような、署名エンベロープ10を作成してこれをクライアント・アプリケーション2に渡す (または使用できるようにする) 。

クライアント・アプリケーション2が署名の確認を望むときには、これはその署名エンベロープ10を署名確認モジュール6 (署名確認サービスともいわれる

)に渡す。署名確認モジュール6は、その署名の署名情報とその署名の“所有者”に関する情報のテンプレートを内容とするテンプレート・データベース12(署名者データベースとも呼ばれる)にアクセスし、そして署名対応率をクライアント・アプリケーション2に戻す。

図2は、署名がペン装備のコンピュータで採取されるが、遠隔システムにて確認される構成を示すものである。図2においては、2つのクライアント・アプリケーション2aおよび2bがある。この実施例においては、クライアント・アプリケーション2aはペン装備コンピュータに搭載されている。署名採取モジュール4は署名を採取して署名エンベロープ10をクライアント・アプリケーション2aに戻す。この署名エンベロープ10は別のクライアント・アプリケーション、例えば、クライアント・アプリケーション2bに送ることができる。クライアント・アプリケーション2bは、署名エンベロープ10により提示される署名が確認されることを要求することができる。この場合には、クライアント・アプリケーション2aはその署名エンベロープ10を署名確認モジュール6に渡し、この署名確認モジュール6が上記署名を確認する。

本発明のこのオープン構成は多くの変更形態を可能とすることが注目される。例えば、この署名確認モジュール6とテンプレート・データベース12を単一のコンピュータシステムに搭載することができる。また、多数の署名確認モジュール6を相異なるプラットフォームに搭載して、その全てが遠隔配置された1つのテンプレート・データベース12にアクセスできるようにすることができる。

この署名採取モジュール4と署名確認モジュール6は1組のAPI(アプリケーション・プログラム・インタフェース)を利用して署名の採取および確認を多数の相異なるアプリケーション、例えば、2a、2bに組込むことを可能としている。アプリケーションは各署名の背景や署名確認の識閾(Criteria)を決定することができる。

この代表的な実施例においては、本発明はIBM社(International Business Machines Corp.)のOS/2(C++インタフェース)用のペンおよびマイクロソフト社(Microsoft Corp.)のペン計算[C++およびビジュアル・ベーシッ

ク・インタフェース (Visual Basic Interface)] 用ウィンドウズにおいて実施される。署名採取モジュール4および署名確認モジュール6は別のコンピュータプログラムに組込まれるか、あるいは別のコンピュータプログラムにより作動されるように指定されている。したがって、これらは自給式ソフトウェア構成要素と考えるべきである。

この代表的な実施例においては、署名採取モジュール4は図式ディスプレイ装置およびディジタイザの両者の利用性を要件とする。ペン計算およびOS/2用のペン用の両ウィンドウのもとでは、その動作システムにより支援される図式ディスプレイ装置はいかなるものも使用され得る。例えば、ワコム (Wacom)、カルコンプ (Calcomp)、クルタ (Kuruta) 等が使用可能である。加えて、このコンピューター・プロセッサは、例えば、コンパック (Compaq) のコンサート

・コンピュータ (Concerto Computer) またはIBMのPシリーズ・シンクパッド・コンピュータ (P.Series Thinkpad Computer) のような動作システムのいずれか一方を支援するペンベースのコンピュータとすることができる。

署名確認モジュール6は、特定のハードウェアを要件とせず、この代表的な実施例においては、C++コンパイラまたはクロス・コンパイラを支援するコンピュータ動作システムのもとで実施することができる。

本発明は次の3つの分離可能なサブシステムを持つと考えることができる。即ち、

1. 署名採取モジュール4 ; これは署名エンベロープ10に署名して同署名エンベロープを作成する行為を記録する。
2. 署名確認モジュール6 ; これは個人の署名プロフィール、即ち、“テンプレート” に基いて署名エンベロープを測定する。
3. テンプレート・データベース12。

これらの3つのサブシステムの用途を示すためには、コンピュータシステムへのアクセスを統制すべく署名確認の単純な適用を考慮することが必要である。この場合のクライアント・プログラム2は署名の採取を要望し、ついで、これを確認してコンピュータ・ユーザーの身元に関する証拠を受取る。この場合、そのス

テップは次の通りである：

- * ユーザーが主張する身元を確定する。
- * ユーザーの署名をその日時と共に採取する。
- * ユーザーが主張する身元を使用してその署名テンプレートの場所を確定する。
- * その署名がそのユーザーのテンプレートに対応しているか否かを確定する。

これらのステップは、上記3つのサブシステムとの関係において次のように説明することができる：

- * ユーザーが主張する身元を確定した後、そのユーザーの識別子を有する空のエンベロープを作成する。
- * 署名採取モジュール4をして署名データを収集させて、その日時と署名の理由の文字通りの表現と共に署名エンベロープに入れる。
- * 署名確認モジュール6をしてテンプレート・データベース12をサーチさせ、署名エンベロープ10に保存されているその署名者のテンプレートの場所を確定させる。
- * 署名確認モジュール6をして、その署名エンベロープ10が見出されたテンプレートに基いて確認させる。

署名確認モジュール6は、この代表的な実施例においては次のように動作する。各署名の測定（署名エンベロープ10から得られたもの）とその平均（そのテンプレートから得られたもの）との差が計算され、そして記載時に計算される測定のための標準偏差により割算される。その最高結果値が保存され、そして全ての値が総計されて平均化される。最高値と平均値は2つの係数により算定されて比較可能値となし、このうちの最大のものが保持される。もしこれが所定の（小さい）値Mよりも小さければ、最大得点100が戻される。同様にして、もしこれが所定の（大きい）値よりも大きければ、最小得点が戻される。別の手法としては、この結果値をM+1から除算し、その差を100で乗算して0から100までの範囲の値を出す。ついで、この値がクライアント・アプリケーション2に

戻される。

得点をクライアント・アプリケーション2に戻すことは、クライアント・アプリケーション2が特定の処理との関係においてその署

名が合格か落第かを決定できるようにする。例えば、署名されている文書が\$1,000(1,000ドル)のローン文書であれば、合格点として得点75またはこれ以上の得点がクライアント・アプリケーション2により要求される。しかし、署名されている文書が銀行口座から\$200,000を下ろすための下ろし伝票であれば、この場合は、クライアント・アプリケーション2は合格点として得点95またはこれ以上の得点を要求することができる。

この構成を使用して、本発明は手書きの署名の採取と確認が相異なるプラットフォーム上で行えるようにすることができる。本発明は輸送可能なデータ式記録、署名の行為を記録するタイプの輸送可能なデータを創作し、そしてこれが文書とリンク(または“結合”)できるようにする。

本発明は、それぞれにおいて動作が実行されて機構が相互作用を可能とする3つのサブシステムの性質を参照することにより最もよく理解することができる。

1. 署名エンベロープ10

署名エンベロープ10は、署名の物理的行為をデジタル記録するコード化データの複雑な包みとして考えることができる。

しかし、署名の行為は純粹には物理的行為とは考えられない。実際には、このような行為は、署名人の意図、日時、および署名される文書等の一連の関係から分離することはできない。署名エンベロープ10は、これら本質的な付随要素に関するデータもその内容とする。

署名が採取されるに先立ち、署名採取モジュール4は、通常はクライアント・アプリケーション2から、次の情報が与えられる：

* 署名に際してのユーザーの意図の要旨(短いテキストの形

式)；これは署名採取モジュール4により、ユーザーの署名が表示されるコンピュータのディスプレイの領域に近接して目立つ状態に表示される。この短いテキ

ストは「重要プロンプト」として知られている。これは署名の行為の重量（重要性）を知らせるからである。例えば、重要プロンプトでは、“私はジョージ ビール（George Beals）に\$49,500支払うことに同意する”、または“私は私の家をフレッド デニング（Fred Denning）に\$23,000で売ることに同意する”、または“あなたは「手紙」という名称の文書に署名しています、ファイル名はlet.wp”、または“クレジット契約書に同意の署名をして下さい”と書くことができる。

* 任意ではあるが、ユーザーが署名する文書を示すコンピュータ・ファイルの参照。

* 任意ではあるが、署名の可視表示が署名エンベロープ10の内側に保存されるべきか否か。

* 任意ではあるが、保全のための検査合計値の生成にキーを使用するか否か。

署名採取プロセスが開始すると、用紙またはウインドウ20（図3に示す）がコンピュータのスクリーンに表示され、そして重要プロンプト22が署名採取モジュール4により表示される（図3において、重要プロンプトには“登録が不完全—登録のための署名をして下さい”と書かれている。この重要プロンプトは、以下に詳しく説明するが、テンプレート作成時の登録プロセスにおいて使用され、ユーザーに彼がテンプレート作成のための署名をしていることを知らせる）。ユーザーはいつでも用紙上に表示の“取消し”制御部24を作動させることで、即ち、これを彼のペンでたたくことでその処理の取消しを選択することができる。

ユーザーはまた、“クリア”制御部26を同様に作動させること

により署名の採取（例えば、腕を揺することによって）を再度開始することもできる。ユーザーが“OK”制御部28を作動させれば署名の採取は完了するが、これは次の仕様に基くものである：

* 署名は完了まで一定の時間を要するものでなければならない。

* 引く線の長さは一定の最小限度よりも長くなくてはならない。

- * 署名データは一定の複雑さを提示するものでなければならない。

- * ペンは2秒以上静止してはならない。

これら仕様のいずれかに違反した場合には、署名者にメッセージが表示されてその署名は拒絶され（ユーザーが“クリア”制御部26を操作したと同様）、システムは自動的に別の署名を受入れる状態となる。

この時点で署名採取モジュール4は署名エンベロープ10に次の情報を保存する：

- * 署名の行為の日時。

- * 重要プロンプト。

- * 署名人が主張する身元。

- * 署名が採取された機器の身元。

- * 署名の採取を開始したコンピュータ・プログラムを代表する確認者、即ち、クライアント・アプリケーション2。

- * 署名に関する測定および統計、例えば、形、ペンの筆跡、署名に要した全時間等。

- * 任意ではあるが、採取された署名が関係するファイルまたは文書として、照合が最初に指定されたコンピュータ・ファイルまたは文書メントから計算される検査合計値(checksum)。

- * 任意ではあるが、署名のイメージをベクトル形式で圧縮した表示。

- * 保全のための検査合計値(checksum)。

本発明は署名採取後の署名エンベロープ10の変更を許可しない。署名エンベロープ10に保持されたデータはコード化に先だって合計チェックが為されて、未公認の修正が検知できるようになっている。

図3Aに示すように、クライアント・アプリケーション2は署名採取モジュール4に、署名されている文書の身元および、またはその文書が署名されている理由（または重要性）を供給することができる。この情報が重要プロンプト22である。この代表的な実施例においては、重要プロンプト22は署名採取ウインドウ20においてユーザーに表示されている。これによってユーザーは、署名して

いる文書は彼または彼女がいまこれに署名しているのだと信じる文書であることを確認することができ、更に署名の行為のグラビティ（重み）の理由を認識することができる。この代表的な実施例においては、重要プロンプト22は署名エンベロープ10に保存される。したがって、この重要プロンプト22は後の段階で別のアプリケーション（これらは別のプラットフォームで操作することができる）により回復されて表示することができる。図3Aに示すように、署名されている文書は全5頁の消費者クレジット・アプリケーションであり、その一部がウィンドウ30に表示されている。署名されている文書のタイトルは文書用のタイトル・バー32においてクライアント・アプリケーション2により表示される。重要プロンプト22には、“クレジット契約書（合意書）承認の署名をして下さい”と書かれている。このテキスト“クレジット契約書承認の署名をして下さい”は、クライアント・アプリケーション2が署名採取モジュール4に供給したものであり、このテキストは署名エンベロープ

10に保存される。署名採取ウィンドウ20は、図3Aにおいて、署名されている文書を内容とするウィンドウ30に表示されている。

本発明（この代表的な実施例においては、署名確認モジュール6は下記の機能を実行する）は、クライアント・アプリケーション2の要求がある場合、署名エンベロープ10に関連して次の機能を提供する：

- * 署名人が主張する身元の開示。
- * 署名の行為の日時の開示。
- * 署名が採取されたときに文書の合計データの検査の選択が実行された場合に、文書を代表する所定のコンピュータ・ファイルが、最初に検査合計値のチェックがなされたものと同じか否かの確認。
- * 署名が採取された場合、その署名の可視表示の保存の選択が実行されたときに、その署名をコンピュータのスクリーンに表示できること。
- * 署名が採取された場合、その署名の可視表示の保存の選択が実行されたときに、その可視表示を内容とする標準フォーマットのディスク・ファイルをビット・マップ形式で生成できること。

* テンプレートに基く確認。

加えて、本発明は、署名エンベロープ10に関連して次の機能を実行することができる：

* 保管、または遠隔システムへの送信を可能とするために、メモリからデータ・ブロックへのコード化。

* アーカイブ（保管所）から、または電子的データ送信を介して回復されたデータ・ブロックからメモリにおける署名エンベロープ10の作成。

メモリから回復されるデータ・ブロックは最初に出されたオブジェクトと同一のオブジェクトを再構成するに足るデータを内容とする

する暗号ブロックのメモリである。データ・ブロックは、オリジナル・オブジェクトの全状態を保存し、且つ同じまたは遠隔システムで再生できるようにするブロック情報であって、効果的にコード化され、そしてポータブルのものである。

これらのデータ・ブロックは、オブジェクトを保管所に保管するために、あるいはオブジェクトのコピーを遠隔システムに送信するために使用される。本質的にはこれらデータ・ブロックはオリジナル・オブジェクトと同じ情報を内容とするが、このデータ・オブジェクトが後日同じデータ・ブロックから再構成できるように高度に構築された形式で表現される。

この代表的な実施例においては、署名エンベロープ10はソフトウェアオブジェクトとして圧縮される。典型的な署名エンベロープのソフトウェアオブジェクトの表示は次の通りである：

データ

署名エンベロープの版番号

機器の連続番号

機器のブート時間

機器のタイプ（番号）

主張された身元（採取アプリケーションにより認識された署名者を確認する一連の文字）

ヘッダ・テキスト（可変長さのASCIIテキスト）

署名人の外観ファイル検査合計値の圧縮表示

キーが施された保全用の内部検査合計値

方法

- 採取する : UI構成要素を表示し、署名を収集する
- 表示する : 採取した署名のイメージをディスプレイ上に描く
- tiffファイルに書込む : イメージをTIFFフォーマット・ファイルに書込む
- win bmpファイルに書込む : ウインドウ・ビットマップ・フォーマットに書込む
- os2 bmpファイルに書き込む : OS/2ビットマップ・フォーマット・ファイルに書込む
- 採取される : 署名エンベロープ10が署名を内容とするか否かを報告する
- イメージを持つ : 署名エンベロープ10がイメージを内容とするか否かを報告する
- 機器の連続番号 : 採取機器の連続番号を報告する
- 機器のタイプ : 採取機器のタイプを報告する
- 署名時 : 採取の日時を報告する
- 主張される身元 : 主張される身元の索線を報告する
- 重要プロンプト : 重要プロンプトを報告する
- ファイルを確認する : 保存された検査合計値に基いてファイルの内容をチェックする
- 移入する (Import) : コード化されたデータ・ブロックからデータを書込む
- 移出する (Export) : コード化された内部データでデータ・ブロックを書込む

本発明の署名エンベロープ・オブジェクトの典型的なライフサイ

クルは図 4 にフロー・チャート形式で要約されており、これを以下詳細に説明する。

生成（ステップ 100）

ソフトウェアオブジェクトが生成される時には、これは署名の採取が開始される状態に初期化される。

採取／移入

採取（ステップ 102）

採取プロセスにおけるイベント（Event）のシーケンスは図 5 にさらに詳しく示されている。採取ステップ（102）は、この代表的な実施例においては、署名採取モジュール 4 により実行される。

署名エンベロープ 10 のオブジェクトが前もって採取された場合には、採取の要求は否定される。

クライアント・プログラムは、重要プロンプトが表示されるべく、署名イメージが保持さるべきか否か、および、文書綴じのために文書の検査合計値のチェックがなされるべきか否かを指定する。

文書の検査合計値のチェックがなされる場合には、その文書が保存されているファイルが熟読されて検査合計値が確立される。本発明の代表的な実施例は RSA 社により公開されているような文書の検査合計値チェックのためのメッセージ・ダイジェスト技術を使用する。

ついで、ユーザー・インタフェース構成要素がコンピュータのグラフィック・スクリーンに顕著な状態で表示され、確実かつ拘束力ある署名が採取されねばならないという事実に注意を喚起する（例えば、図 1 参照）。

ユーザーが“取消し”制御部 24 を操作した場合には、適切なる

状態がクライアント・プログラムに戻される（ステップ 202 および 204）。

ユーザーが“クリア”制御部 26 を操作した場合には（ステップ 206）、先に収集されたペン・データが破棄されて放棄された署名はディスプレイからクリアされる（ステップ 208）。

ユーザーがペンを署名採取領域で操作すると（ステップ 210）、ペンの動き

を表すデータが収集されてメモリに保存される（ステップ212）。ユーザーが“OK”制御部を操作すると（ステップ214）、署名採取モジュール4が採取したペン・データを分析して特定の測定を記録する。この代表的な実施例においては、署名採取モジュール4が実行する測定は次の通りである：

M0	ストローク数
M1	全時間
M2	ペンが下っている時間
M23	線の全長
M23/M0	平均ストローク長さ
M2/M0	ペンが下っている時間/ストローク数
M1/M23	平均速度
	各ストロークにおける最低速度点の時間の総計
	各ストロークにおける最高速度点の時間の総計
M34	各ストロークにおける最低速度点の位置の総数
M35	各ストロークにおける最高速度点の位置の総数
M36	ペンが下っている位置の総数
M37	ペンが上っている位置の総数
M38	加速および減速の最大（「イベント」）の数
M40	イベント位置の総数
M41	イベント時間の総計
	ペンが下がっている時の平均時間
	ペンが上がっている時の平均時間
M35/M1	最高速度点の時間のねじれ
M37/M23	ペンが上がっている位置の縮尺総数
M23/M38	平均加速/減速
	距離
M39/M23	イベントの期間の総計/線の全長
M40/M1	イベント時間のねじれ

M 4 1 / M 3 8 イベントの平均時間

-ve / +vd の Y 方向距離

+ve / -ve の X 方向距離

Y 方向距離 / X 方向距離

最大 X / 最大 Y

Y 方向距離 / (最大 Y + 1)

Y 方向転向の数、幅 > 0. 8 mm

純領域

速度デルタの差の総数

任意ではあるが、ペン・データは時間情報なくして圧縮され、ベクトル化されて、コンピュータ・ディスプレイ・スクリーンまたはビットマップ・ファイルへの署名のイメージとするために保存される。署名の日時、機器の詳細および重要プロンプトも同様に保存さ

れる。ついで、データブロックの検査合計値が生成されてその後の変更を防止する（ステップ 216）。

本発明は内蔵の保全チェックを含み、これは次のように説明することができる。コード化に先だって、署名エンベロープ 10 の内容は、クライアント・アプリケーション 2 により提供されるキーと共に、ファイルの検査合計に使用したのと同じ技術で検査合計値がチェックされる。したがって、署名エンベロープ 10 を構築させたときのオリジナル・クライアント・アプリケーション 2 が使用するキーを知らずして署名エンベロープ 10 を修正して満足のゆく検査合計値を再生成することは不可能である。保全のチェックを実行するときにこの訂正キーを提供することでクライアント・アプリケーション 2 は（このキーが開示されていなかった限り）署名エンベロープ 10 は解読、修正および再コード化がなされなかったことを保証することができる（ステップ 104）。

先に採取された署名データはメモリ・ブロックから解読されてデータ構成に適切に保存される。

データアクセス（ステップ 106）

本実施の形態において、データアクセス機能は署名確認モジュール6によって行われる。

移出（エクスポート）

署名エンベロープ10内のデータは、メモリ・ブロックに記憶され、コード化される。

署名画像（署名イメージ）をコンピュータ・ディスプレイ上で表示すること（Render）

署名イメージが、本来エンベロープを採取したクライアント・プログラム2によって要求されなければ、表示を要求するクライアン

トはエラー状態に戻る。

クライアント・プログラム2が署名イメージを要求すれば、署名イメージは適当な寸法で表示される。

ビットマップ・ファイルの作成

ビットマップ・ファイルは、標準的なイメージファイル・フォーマットを用いて作成される。本発明の実施の形態に用いられるフォーマットとして、以下に示すフォーマットが推奨される。

T I F F

O S / 2 ビットマップ

ウィンドウズ（Windows）・ビットマップ

クライアント・プログラムからの要求に応じて、本発明のシステムは、以下の事項に関する復号情報をクライアント・プログラムがアクセスできるメモリに配置する。

要求ID（アイデンティティ：Identity）

署名の日時

移出されたデータ・ブロックのサイズ

署名エンベロープ10が採取署名を含むか否か

署名エンベロープ10が署名イメージを含むか否か

署名が採取された機器のシリアル番号

署名が採取された機器の型を示す番号

重要プロンプト

内蔵保護チェックが成功したか失敗したか

署名を採取したとき、付与されたファイルが元々チェック済みと判断されたファイルと一致するか否か

破壊（ステップ108）

依存データの割当ては、破壊される。

2. テンプレート

テンプレートは、クライアント・プログラム2によって直接扱えないが、その代わり、テンプレートのデータベースを実施するソフトウェアの構成要素の媒体を介してアクセスされる。

まず、テンプレートが作成されると、テンプレートはブランクである。本発明によって、クライアント・プログラム2はテンプレートを検知し、連続する署名エンベロープ10を用いてテンプレートを“満たす”ことができる。このプロセスは、“登録”として知られているように、一般的な署名実行者の動作および署名実行者の動作が最適に首尾一貫していることが決定される間の学習プロセスに相当する。

登録段階の間、受け取られた署名エンベロープ10同士がどの程度類似しているかが、最終的なテンプレートの質に影響する。署名エンベロープが全く異なる場合、確認は不可能になり、登録プロセスは始めからやり直される。署名エンベロープが同じ場合、登録の間に受け取られた署名エンベロープがどの程度一致しているかが、確認スコアを考慮して確められる。一致の程度が高いほど、確認プロセスの信頼性は高くなる。

テンプレートが完全であることは、セキュリティを意識したアプリケーション・プログラムにとって非常に重要なので、テンプレートは“所有”アプリケーションに関する情報を含む。テンプレートの所有者のみが、その情報に対して敏感に対応して操作を行うことができる。

テンプレートは、以下の情報を記憶している。

- ・署名計測値と統計値との平均値
- ・これらの統計値の可変量の表示
- ・登録の状態および質の表示
- ・署名エンベロープ10が一番最近に確認された日時
- ・パフォーマンス表示
- ・“所有”プログラムのID
- ・作成日時
- ・独自の識別子

本発明は、テンプレートに関連する以下の機能を提供する。

- ・作成日時の開示
- ・登録の状態および質の開示
- ・署名エンベロープ10の登録（所有プログラムのみ）
- ・強制再登録（所有プログラムのみ）
- ・署名エンベロープ10の確認

確認手順は、クライアント・プログラム2にスコアフォームで偽の署名である可能性を示すのに役立つ。このスコアは、多くの場合登録の質に関する情報とともに、クライアント・プログラムがその判断基準に基づいて署名を許可できるかどうかを決定させることができる。

時間がたつにつれて個々の署名が徐々に変化するので、本発明は、ある環境において、署名動作が一貫して変化するように署名エンベロープ10を“ベンディング (Bending) する”。この「ベンディング」とは、ある内部チェックに基づいて行われ、クライアント・アプリケーションによって選択的に抑制できる。確認される署名エンベロープ10が、ひき続いて確認される最新の署名エンベロープ

よりも古い場合、再び「ベンディング」は行われない（図6のステップ318を参照、詳細は以下に示す）。

本発明の本実施の形態において、各テンプレートはソフトウェアのオブジェクト

トとして実行される。テンプレートのソフトウェアオブジェクトの一般的なライフサイクルの概要は、図6のフローチャートに示され、詳細は以下に記載される。

作成 (ステップ302)

テンプレートのソフトウェアオブジェクトが作成されると、登録、移入（インポート）または移出が初期化できる状態に初期化される。

登録 (ステップ310)

本発明は、テンプレートが非登録状態にある場合のみ、テンプレート登録ができる。登録プロセスの概要は、図7のフローチャートに示される。

署名の所定の最小値は、本発明のシステムが登録を終了させようとする前に、提示されなければならない。この時点に到達するまでは、連続する署名エンベロープ10からのデータは、不完全なテンプレートとともに記憶されるだけである（ステップ402）。

いったん署名エンベロープの最小番号が受け取られると（ステップ406）、本発明はチェックを行い、提示された署名エンベロープがテンプレートを作成するのに十分一貫しているかどうかを決定する。もし、十分一貫していなければ、すべての署名エンベロープは消去（クリア）され、テンプレートは初期状態に再設定される（ステップ414および420）。他方、もし提示された署名エンベロープが十分一貫していれば、テンプレート統計値が発生し（ステップ408）、記憶された署名エンベロープは不要になり、テン

プレートは登録完了のマークが付けられる。

しかしながら、署名エンベロープの最小番号が受け取られ、テンプレートの改良が許可されると（ステップ416）、さらに所定の最大値までの署名エンベロープが受け入れられる。もっとも一致する設定は、良好な登録が確立できるまでまたは最大値に達成するまで保持され、どちらが早くてもよい。

移入 (ステップ304)

予めコンパイルされたテンプレートデータは、メモリ・ブロックから復号され、データ構造に適切に記憶される。

移出（ステップ320）

テンプレートデータは、リモートシステムに到達または伝送されるためにメモリ・ブロックでコード化される。

確認（ステップ314）

署名確認モジュール6は、テンプレートが登録状態のときのみ、テンプレートに対する署名エンベロープ10の確認が行われる。

署名採取プロセスの間に計測され、署名エンベロープ10に記憶された計測値は、テンプレートに記憶された中間値と比較される。登録プロセスの間監視が行われながら、ユーザーの変量がカウントされる。2つの数値が発生し、1つは、中間値からの平均エラーを示し、もう1つは中間値からの最大の分散値を示す。それから、これら2つの値の機能が用いられ、0...100の範囲でスコアが作成される。ここで、0は署名エンベロープとエンベロープの不一致を示し、100は署名エンベロープとエンベロープの一致を示す。

す。署名確認モジュール6のこの特徴の詳細については、前述のとおりである。

クライアント・アプリケーションが確認のための署名エンベロープ10を提供するとき、テンプレート更新のための低しきい値として作用するスコア値も提供する。テンプレートの更新（または「ベンディング」）（ステップ318を参照）は、以下の条件を前提として行われる。

- ・ 確認スコアは、しきい値以上の値である。
- ・ 確認値は、中間値に近すぎることなく、遠すぎることもない値である。
- ・ 署名エンベロープ10は、以前に確認された署名エンベロープ10より最近のものである。
- ・ 確認スコアは、クライアント・プログラム2によって提供されたしきい値より高い値である。

以上の条件を満たせば（ステップ316）、テンプレート内に記憶された中間値が訂正され、ある時間にわたって、テンプレートはテンプレート署名実行者の操作の流れに順応する。更新が行われると、テンプレートにタイムスタンプが行われ、複数または遠隔のテンプレートのコピーの管理が容易に行われる。

消去（ステップ312）

本発明によれば、テンプレートを再登録可能な状態にできる。作成日時は保持され、テンプレートの更新日時は、登録状態においてデータアクセスの現日時に設定される（ステップ306）。テンプレートが登録されたかどうかの調査に応じて、システムは情報のブロックを終了させる（以下に示す）。これはクライアント・プログラム2による調査に利用できる。

本実施の形態において、情報のブロックは、以下のような構成である。

- ・ update_time 統計値が最近更新された時間
- ・ backup_time テンプレートが最近バックアップされた時間
- ・ count 登録を終了させるために用いられた署名の番号
- ・ enroll_state 登録の一致を示す番号
- ・ enroll_flag 登録が完了すると、非ゼロ値を示す

3. テンプレート・データベース12

署名テンプレートは、個々独自のものである。いったんテンプレートが構成されると、そのテンプレートを用いて個人を確認し、ユーザーが本発明のシステムを用いて署名した文書が本物であると認める。明らかに、個々の署名は、1つ以上のクライアント・プログラム2または1つ以上の構成に関連する。テンプレートデータベース12は、1つ以上のアプリケーション2に利用できるように設計されている。このため、確認をする目的で、所有テンプレートまたは登録テンプレートを他のクライアントに用いることによって、テンプレートの“所有者”は、所有テンプレートまたは登録テンプレートから商業的な利益を得る。

テンプレートデータベース12のデータベース構築は、以下の目的に基づく。

・ データベースサービスを利用する前に、クライアント・アプリケーション2は、システムによって作成された特定の識別子を用いて本発明のシステムに確認されなければならない。特定の識別子は、あるアプリケーションが本発明のシステムに登録されるとき、作成される。クライアント・アプリケーションがテンプレートを作成す

る前に、登録を行う必要がある。

- ・ テンプレートが作成される場合、個人名およびユーザー独自の確認番号（例えば、国民健康保険番号または社会保険番号）を含むデータベース記録も作成され、以下、修正できない。この記録を用いて、クライアント・アプリケーションの様々な識別子を同一個人に一致させる。

- ・ 本発明のシステムは、合致データのいかなる組み合わせに対してテンプレートデータベース12をサーチし、あるテンプレートと合致すると関連づける。

- ・ テンプレートを作成する場合または特定のサーチパターンに合致する場合において、本発明のシステムは、クライアント・アプリケーション2に個々のアプリケーション独自の識別子を登録する能力が付与される。以下、クライアントは、好適な識別子を提供しさえすればよい。これは、クライアント・プログラム2が常に署名が確認される個人に関連する独自の識別子のインデックスを有することを認識する。

- ・ クライアントのインストールが適正な使用許諾権を有する場合、本発明のシステムは、別に記録したり伝送するために、テンプレートの記録を、コード化されたデータ・ブロックに変換する。

本発明の構造は、署名確認部の新しい概念に役立ち、いかなる数のクライアント2に対しても遠隔またはネットワークでの確認サービスを提供する。

本発明のシステムは、署名テンプレートのリモートメンテナンスまたはリモート管理にも役立つ。これは、中央部に構築されたテンプレートが中央データベースから独立して“オフライン”確認を行うリモートプロセッサに分配される必要がある場合、非常に重要で

ある。その例として、スマートカード、または小型携帯ペン操作式コンピュータの“フリート（Fleet）”の利用を含み、ここで署名テンプレートの中央集中記憶装置は、正確なセキュリティ構成を用いてフィールド内の装置の欠陥処理およびその欠陥の迅速な交換を行うために重要である。

テンプレート・データベース12の目的は、アプリケーション・プログラム（例えば、2b）が必要とする全てのテンプレートを記憶することである。しかし

ながら、テンプレート・データベース 12 特有の構造は、それぞれ異なるアプリケーションが 1 つのテンプレートを共用できるように、個別のテンプレートを 1 つ以上のアプリケーションに利用させることである。

これは、データベース機能が利用できるようになる前に、強制的にクライアント・アプリケーション 2 がデータベースセッションを開始させることによって、達成される。セッションが開始されると、クライアント・アプリケーション 2 は、その確認を明らかにしなければならない。

データベース 12 は、独自の確認情報とともにテンプレートを示すために個人の概念を用いる。データベース 12 内に記憶された全てのテンプレートは各人に属し、どの個人もアプリケーションのいずれかに登録される。いずれか 1 つのアプリケーションはそのアプリケーションに登録された個人を多数有し、いずれか 1 人の個人はアプリケーションのいくつかに登録される。これは、図 8 のエンティティ関係図に示される。

まず、他のデータベースサービスが利用できるようになる前に、クライアント・アプリケーション 2 はシステムに認知されなければならない。アプリケーション 2 がセッション (Session) を開始すると、アプリケーション 2 は他のすべてのアプリケーションに認知

されることによって、アプリケーション 2 自身を表すパブリックネームを明らかにする。アプリケーション 2 は、シークレット暗号キーも提供する。このキーは本発明によって用いられ、AID として知られるアプリケーションの独自 ID を作成する。同時に、テンプレートにアクセスするとき、個人を確認するために用いられる独自の識別子の長さに関する情報も提供する。クライアント・アプリケーション 2 がテンプレートを作成することを必要とする場合、まず他のアプリケーションに既に登録されている個人のデータベース 12 を走査する。ある個人が登録されると、テンプレートが作成され、他の情報 (氏名、ユーザー ID 番号) も記憶される。このため、これらの判断基準を用いるアプリケーションは、当該個人がクライアント・アプリケーション 2 に既に登録されているか否かを決定できる。

もし合致する個人が見つからなければ、新しい個人データが作成され、データベース12に追加される。

本実施の形態において、個人はソフトウェアのオブジェクトによって示される。この個人に関するソフトウェアオブジェクトのライフサイクルは、図9に示される。データベース12は、個人のオブジェクト操作を介してクライアント・アプリケーション2の代わりにすべてのテンプレート操作を行う。

ある個人は、その個人に対応するテンプレートとともに、テンプレートを作成するアプリケーション2によって“所有されている”とみなされる。テンプレートの登録およびクリアを含むテンプレートに対する操作は、所有アプリケーション2によってのみ行われる。しかしながら、所有アプリケーションは、他のアプリケーションがテンプレートのロック解除のために用いるパスワードを特定することによって、登録を他のアプリケーションに利用する。

ある個人に関連する名前および独自のユーザーID番号を独自に

用い、全てのアプリケーションにわたってその個人を確認する。その結果、これらのデータは不変である。

個人をアプリケーションに登録する

いったんある個人データがアプリケーション2によって作成され、配置されると、アプリケーション2はその個人をアプリケーション2そのものに登録できる。これは、アプリケーションの独自の個人識別子（一般的に、その個人を確認するためアプリケーションによって用いられる独自のキー）を供給することによって、達成される。独自のキーの長さは、そのキーがまずデータベース12に登録されたとき、アプリケーション2によって明らかにされる。この識別子は、アプリケーション独自の識別子（AUID）として知られ、以下、このAUIDは、個人またはその個人のテンプレートを確認するためのアプリケーションによって用いられる。

登録の際、本発明はAUIDを含む新しいデータベース記録を構成し、アプリケーションを用いて、新しい記録と以前に記録された登録とをリンクさせたり、他のアプリケーションを用いて、新しい記録とその個人に関する以前の登録とを

リンクさせる。

アプリケーションは、以下に関するデータベースを走査する。

- ・ 全てのアプリケーション
- ・ アプリケーションに登録された全ての個人
- ・ アプリケーションに登録されていない全ての個人
- ・ 合致判断基準に合う全ての個人

本発明は、図6のステップ310に示すように、時間が経過するにつれて、個々の署名テンプレートをユーザーの署名の変化に応じて“修正する”。例えば、署名実行者が2秒前後で自分の名前を署

名する。これは、およそ1/10秒の範囲で変化し、署名確認モジュール6は、署名実行者の署名に要する時間が2.2秒または1.9秒続くと、“その署名実行者をマーク”しない（すなわち、その署名実行者の署名合致の割合を低下させない）。しかし、数ヶ月後（大抵、ユーザーが用いる装置に慣れていない場合）、ユーザーの署名は、1.9秒でマークされる傾向にある。他の全てのデータが署名実行者の登録に対してほぼ適正なので、署名確認モジュール6は、署名実行者の署名テンプレートをわずかに“ベンド”し、署名実行者の署名操作のパターンまたは変更に従う。1年後、署名実行者は1.8秒でまちがいをなく署名するが、1.7秒または1.9秒かかる場合もある。この時間によって、中間値は署名実行者の操作に従い、1.8秒に設定される。（署名実行者の元の署名の1つが署名エンベロープ10に採取されながら再提示され、その時間が2.1秒かった場合、報知は失敗してしまう）。

ソフトウェアオブジェクト

上述の如く、本発明の代表的実施例はオブジェクト指向のプログラミングテクニックを用いて実現されている。また、以下に列挙するのは、本発明を実現する上で用いられる代表的なオブジェクトである。

4.1 署名エンベロープ・オブジェクト。

これは署名行為を保護するために用いられるとともに、内部的に以下のサブオブジェクトを用いている。

4.1.1 署名イメージを表すオブジェクト。このオブジェクトは、イメージデータと、該イメージデータを移入および移出すると共にビ

ットマップ形態で表示またはディスプレイ装置上にダイナミックに表示する方法とを含むものである。

4.1.2 署名の語句的内容ではなく、署名の行為自体を表すオブジェクト。このオブジェクトは、個々のペンストロークに関する署名の計測値（筆寸）および付随データを含んでいる。このオブジェクトの主要目的は、照合機能により用いられる計測値を表すことである。このオブジェクトはまた、署名採取時に用いられて生のペンデータを記憶するテンポラリ・オブジェクト（Temporary Object）にも関連し得る。

4.1.3 生のペンデータを表すと共に、このデータに対して例えばストローク数、点の数などの基本的な分析を加えるオブジェクトであって、4.1.2のオブジェクトが計測値を作成し得るように生のペンデータへのアクセスを与えるオブジェクト。

4.2 署名テンプレート・オブジェクト

このオブジェクトは、署名エンベロープ・オブジェクト10内の計測値の平均値およびこれらの計測値の標準偏差を含んでいる。このオブジェクトは2つの主要機能を有している。即ち、一連の署名エンベロープから“学習”または“登録”する機能と、登録後に署名エンベロープ10と比較するという機能であり、これは実際には照合機能そのものである。それは、最も直近に署名がなされたエンベロープの作成データおよび作成時刻を除き、いずれの署名エンベロープ10に関して何も保存しない。この情報はクライアント・アプリケーション2から読み出すことができ、したがって、クライアント・アプリケーションは順番外のエンベロープが照合されているか否かを決定することができる。

4.3 テンプレート・データベース・オブジェクト

このオブジェクトは基本的に、署名者のIDに関するテンプレートをコード号化して記憶するに適した手段をクライアント・アプリケーション2に対して与え

るために存在している。

該オブジェクトは2つの主要なサブオブジェクトを含み、それは次のものである：4.3.1 人物に関する基本的情報を保持するとともに、該当人物を参照するアプリケーションにこの情報を交差結合するオブジェクト。該オブジェクトは、アプリケーションデータベースと人物データベースとを2つの結合データベースとともに保持することにより、その機能を達成している。一方の結合データベースは、アプリケーションの各々を該アプリケーションが参照する必要のある人物の全てに対して結合し（この結合データベースは、人物特定時に該当人物に対してアプリケーション自体が使用する特有のIDをも含んでいる）、他方の結合データベースは、該当人物を参照するアプリケーションの全てを人物の各々に対して結合している。

したがって、このオブジェクトの主要目的は、ひとりの人物が、多数のアプリケーションの夫々の目的に最も適した手法でこれらのアプリケーションから参照され得る様にするることである。

4.3.2 人物ごとの固有な識別子によりインデックスを付したデータベース内に実際のテンプレートを保持するオブジェクト。

以上のデータベースオブジェクトは両者ともに、特定のタスクに最も適切なファイルの形式および構造を管理する従属オブジェクトを使用している。例えば、複数の項目列を含む、インデックス付きファイル、シーケンシャルファイルおよび結合リストファイルがある。

尚、本発明のアーキテクチャは、署名以外の生体情報を採取かつ照合するためにも活用し得る。例えば、本発明のアーキテクチャは、指紋情報、眼球パターン情報、および声紋情報を含むエンベロープを作成かつ照合する為にも使用され得る。

例

上述した如く、本発明の代表的実施例における署名採取モジュール4は、署名された文書の検査合計値を作成することができる。この文書検査合計は、署名したものと主張された文書がその署名文書であり、さらに、この文書には何らの変

更も加えられていないことを後日に照合すべく使用されるものである。上記の代表的実施例においては、文書の検査合計はオリジナル文書全体を記述するものでなく、したがって、文書の検査合計値からオリジナル文書を引出すことはできない。また、文書検査合計は文書と数理的な関係を有することから、もし文書に変更が加えられれば検査合計値とは数学的に一致しなくなる。本発明のこの特徴は、署名綴じと称されるものである。以下には、本発明に係る署名綴じの特徴の操作例が示されている。

先ず、以下のサンプル文書が与えられたとする：

“私はボルネオに生まれたことをうれしく思う (I am glad I was born in Borneo. <CR> <LF> ”

これは次のASCIIデータに等しい：

```
49 20 61 6D 20 67 6C 61 64 20 49 20 77 61 73
20 62 6F 72 6E 20 69 6E 20 42 6F 72 6E 65 6F
2E 0D 0A
```

検査合計値はメッセージ圧縮アルゴリズム（例えば、RSA(RSA Security Inc.)により開発されたMD4またはMD5アルゴリズム）

を用いて作成され、例えば次のような（16進の）文書検査合計が作成される：
89F32145AB321AF7C411FB76543F0CFC。

ここで、署名エンベロープは次の情報を含んでいる：

- ・ バージョン番号（整数）
- ・ 機器のシリアル番号（整数）
- ・ 機器のブート時刻（整数）
- ・ 機器とオペレーティングシステムの種類（整数）
- ・ 署名者が主張するID（可変長、キャラクタ）
- ・ 重要プロンプト（可変長、キャラクタ）
- ・ 署名筆寸の列（整数）
- ・ 署名の日付／時刻（整数）

- ・署名イメージ（可変長）
- ・ファイル検査合計（キャラクタ）
- ・エンベロープ検査合計（キャラクタ）

コード化されたデータ・ブロックに移出されるときに、これらの情報には次の長さ情報が加えられる：

- ・エンベロープの合計長（整数）
- ・署名者が主張するIDの長さ（整数）
- ・重要事項の長さ（整数）
- ・署名イメージの長さ（整数、但し、署名がなければゼロ）

上記署名イメージは詳細には次の様にして記憶される：

- ・開始座標値
- ・前の座標値と次の座標値との間の差の列

また、これらのデータ項目の各々は、次のようにして構成される。

もし次のキャラクタを整数として見た場合に負であれば、そのキャラクタの残りのビットは次の条件を表すためのフラグとして用い

られる。

- ・ストロークエンド（End of Stroke）
- ・次の値は2キャラクタ長であること
- ・1つおいた次の値は2キャラクタ長であること
- ・次の値は符号を変えていること（負から正へ、またはその逆）
- ・1つおいた次の値は符号を変えていること
- ・次の値は反復計数値（Repeat Count）（常に正）であること

例えば、署名が幾何学的に鋭角的な文字“V”で始まるとすれば、そのイメージは次のように表される：

1. Y座標値が20であることを示す、正のキャラクタ
2. X座標値が0であることを示す、ゼロキャラクタ
3. 反復回数を表すビットがセットされた、負のキャラクタ
4. 10の値を有するキャラクタ

5. Yが負に変わることを表すビットがセットされた、負のキャラクタ
6. Yの差が2（即ち-2）であることを示す、正のキャラクタ
7. Xの差が1であることを示す、正のキャラクタ
8. 反復回数を表すビットがセットされた、負のキャラクタ
9. 10の値を有するキャラクタ
10. Yが正に変わることを表すビットがセットされた、負のキャラクタ
11. Yの差が2である（ここでは+2）キャラクタ
12. Xの差が1であるキャラクタ
13. ストロークエンドであることを表すビットがセットされ

た、負のキャラクタ。

ここで、クライアント・アプリケーションが、署名を採取して上記のボルネオ（Borneo）文書にこの署名を付加することを企図したとする。OS/2オペレーティングシステムでは、以下の情報が用意される。

—署名採取ウインドウ20が挿入されるウインドウ（例えば図3Aの30）に対するOS/2の識別子、

—署名者を特定する、ゼロキャラクタで終わるキャラクタ列、

—重要事項を与える、ゼロキャラクタで終わるキャラクタ列、

—署名イメージの採取が望まれるのであれば、ゼロ以外の値を有する整数、

—完全性検査合計のためのシークレット・アプリケーションキーを与えるキャラクタ列、

—このシークレットキーの長さを与える整数、および

—検査合計が行われるべき文書を記憶するファイルの名前を与える、ゼロキャラクタで終わるキャラクタ列。

署名採取コンポーネントは次に、適切な重要事項22と、署名者が主張したIDとを伴う署名採取ウインドウ20を表示する。このコンポーネントは指定されたファイルを縦覧して検査合計値をも作成する。この署名採取ウインドウ20上でユーザーがペンを走らせる間、ペンデータは、XおよびYの移動値および時間差の形態で内部的に記憶される。もしユーザーが引続いて“OK”制御部28を

起動すれば、これらの移動値は絶対距離を表すべく縮尺が付けられ、さらに、署名の計測値を求めるべく分析される。最終的に、署名イメージが要求されれば、上記ペンデータはイメージ列に変換される

(タイミング情報の全ては取り除かれる)。

この時点で、クライアント・アプリケーション2には、数字コードにより相互作用の結果が通知される。

0. エンベロープの作成に成功

1. 署名は放棄されたー即ち、ユーザーが“取消し”制御部を起動した
3. 無効な(例えば長さがゼロの)IDを主張した
4. 無効な(例えば長さがゼロの)重要プロンプト
5. 検査合計が行われるべきであったファイルの誤った読み込み

【図1】

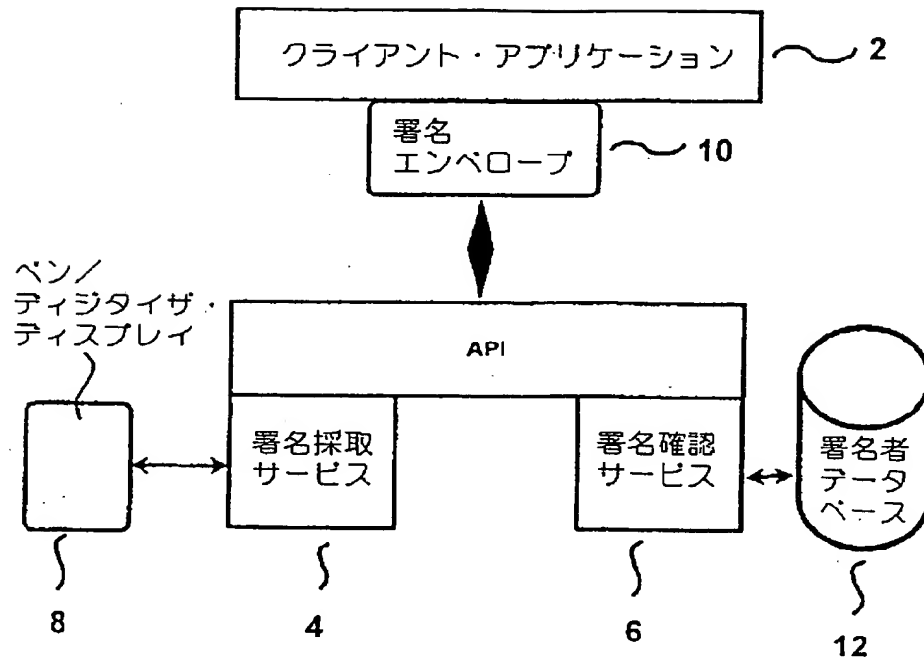


FIG. 1

【図2】

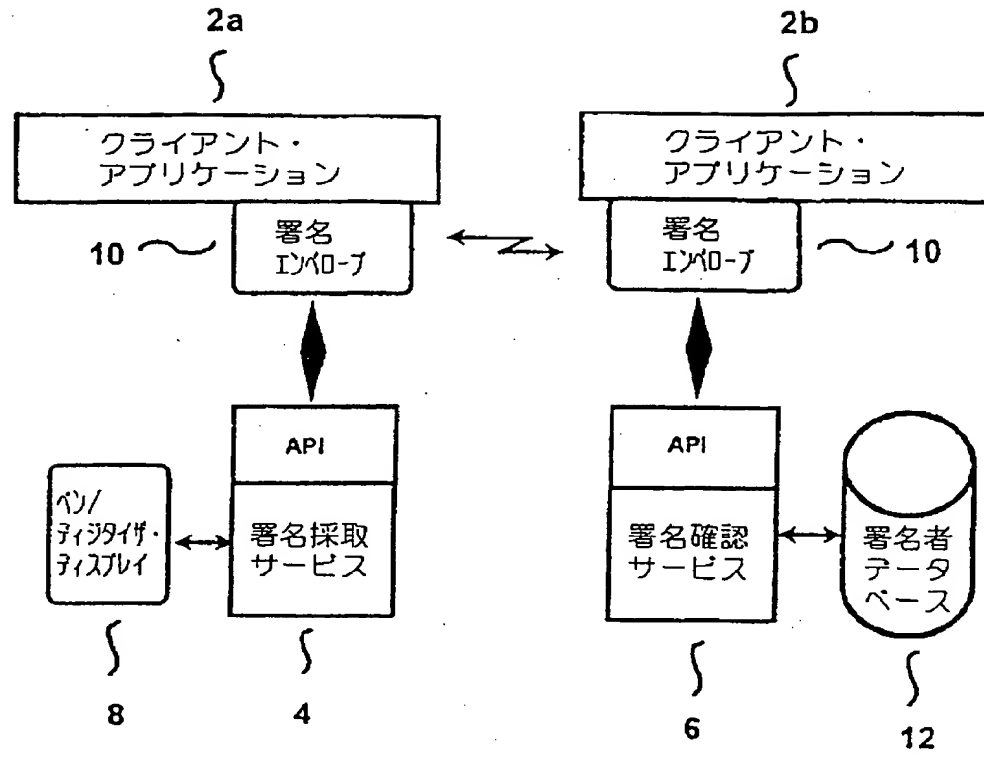


FIG. 2

【図3】

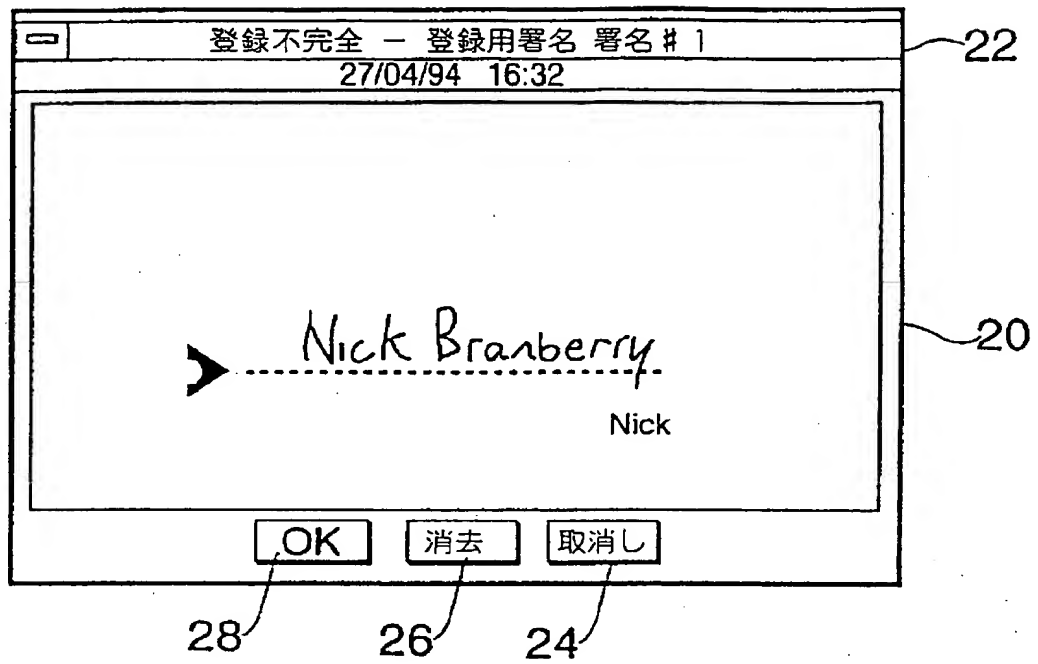


FIG. 3

□

消費者クレジット・アプリケーション (5の5頁)

▽

△

合意書

ここに署名することによって、貴方は、自らがここに記した情報、あるいは今後記すことになるであろう情報の全てが真正かつ完全なものであることを証明します。貴方は、我々に対し貴方の陳述の全てについて任意の情報供給源で確認し、信用および職務経歴を入手し、貴方の信用および信用取引経歴について他者と情報を交換することを許可します。貴方はまた、真正かつ完全な連邦所得税申告書、雇用確認および所得確認を求め（ただし、これに開かれるわけではない）、当該アプリケーションを処理するのに必要となる得る付加的な情報を提供することに同意します。

□

クレジット合意承認署名

17/06/94 11:26

貴方の署名

R. Template

銀行使用専用

Res S / Mktg

コート

販売事務所

販売事務所 I D

204a

CPK Smi

28

26

CPK Smithies

24

OK

消去

取消し

先行

—

関連ボタンをたいて処理を進める

—

終了

【図 3】

FIG. 3A

【図4】

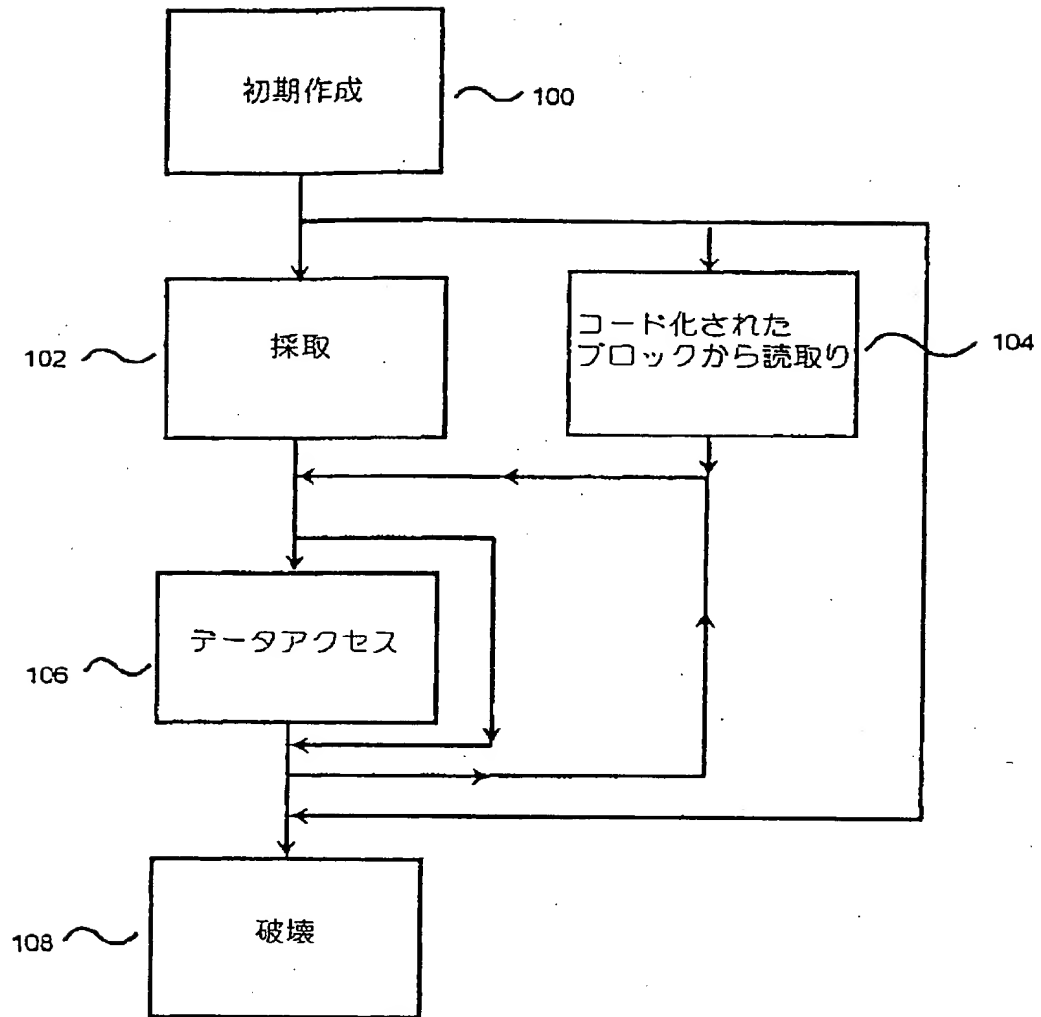


FIG. 4

【図5】

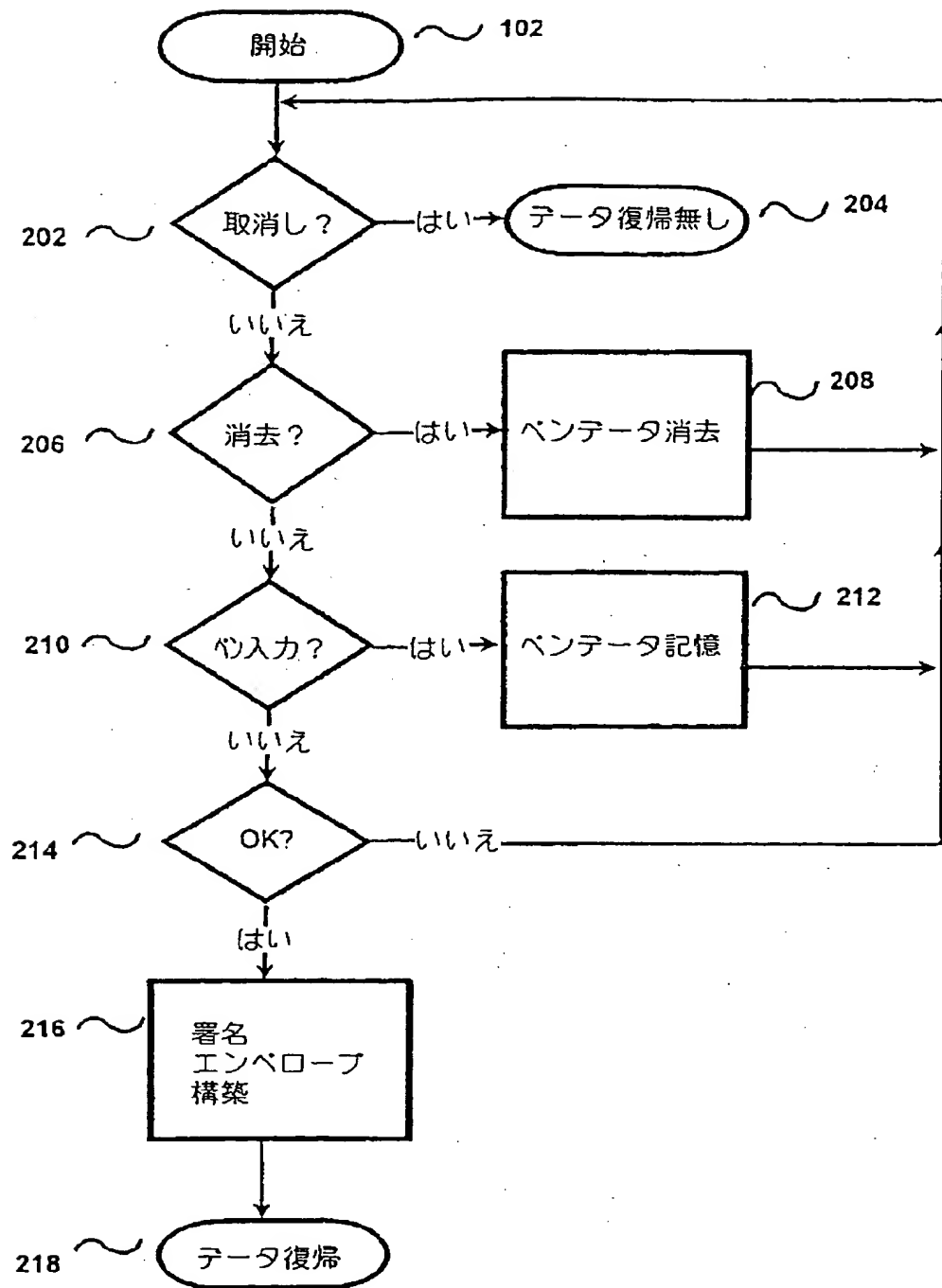


FIG. 5

【図6】

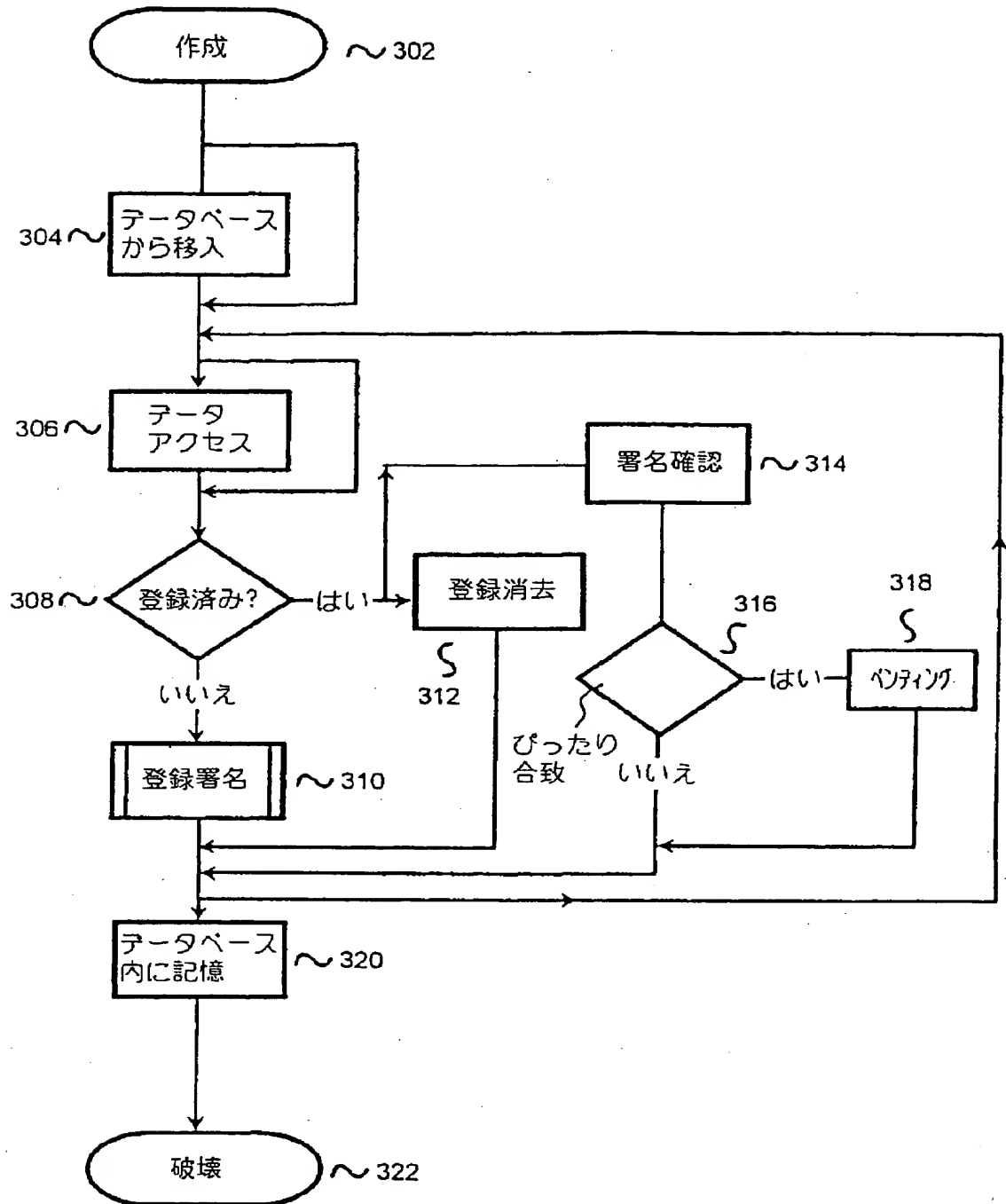


Fig. 6

【図 7】

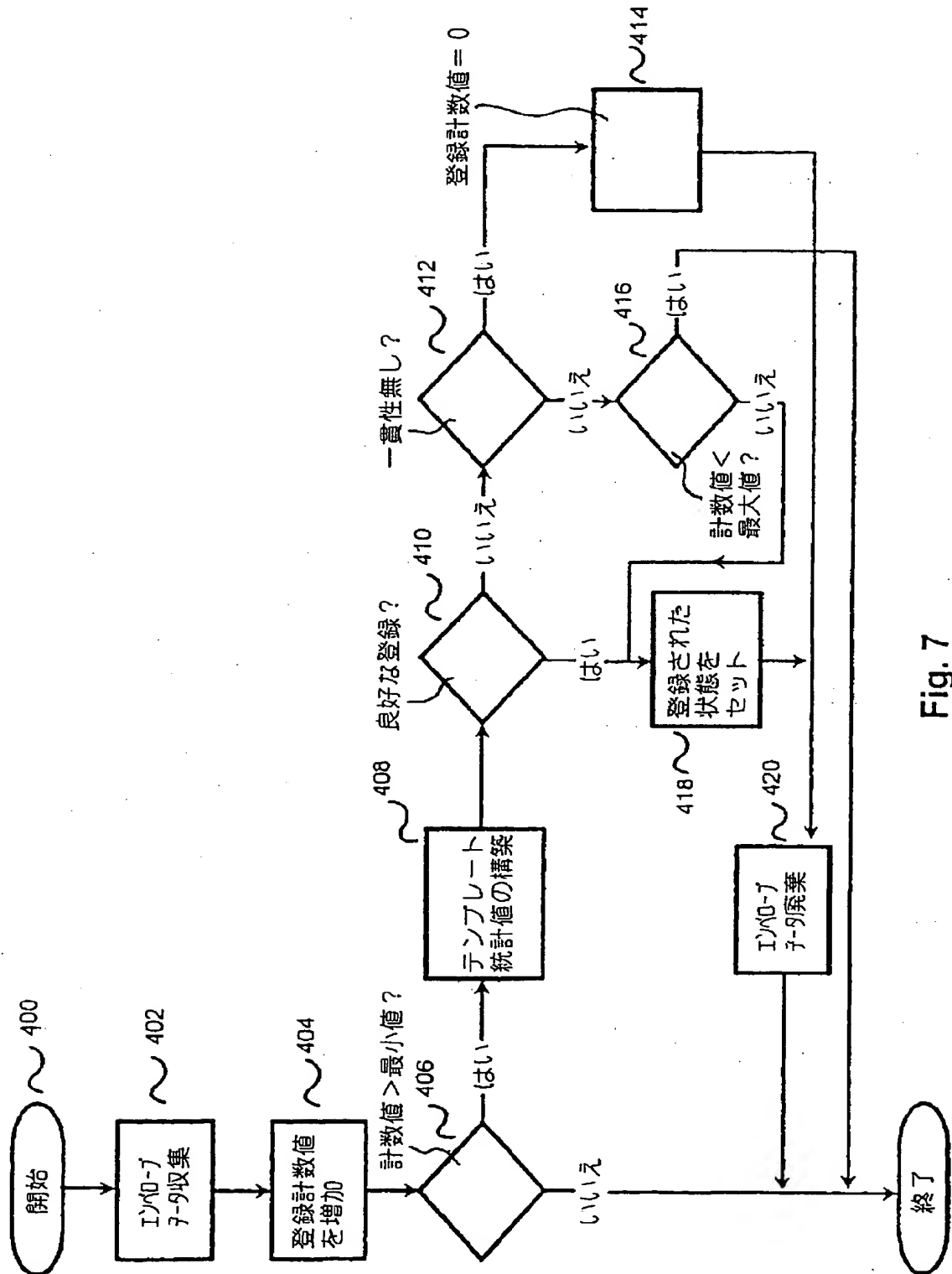


Fig. 7

【図8】

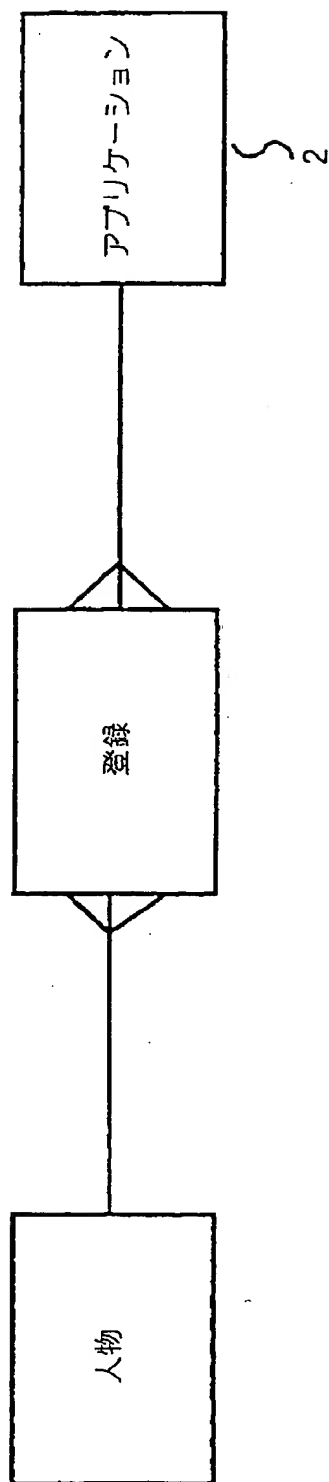


Fig. 8

【図9】

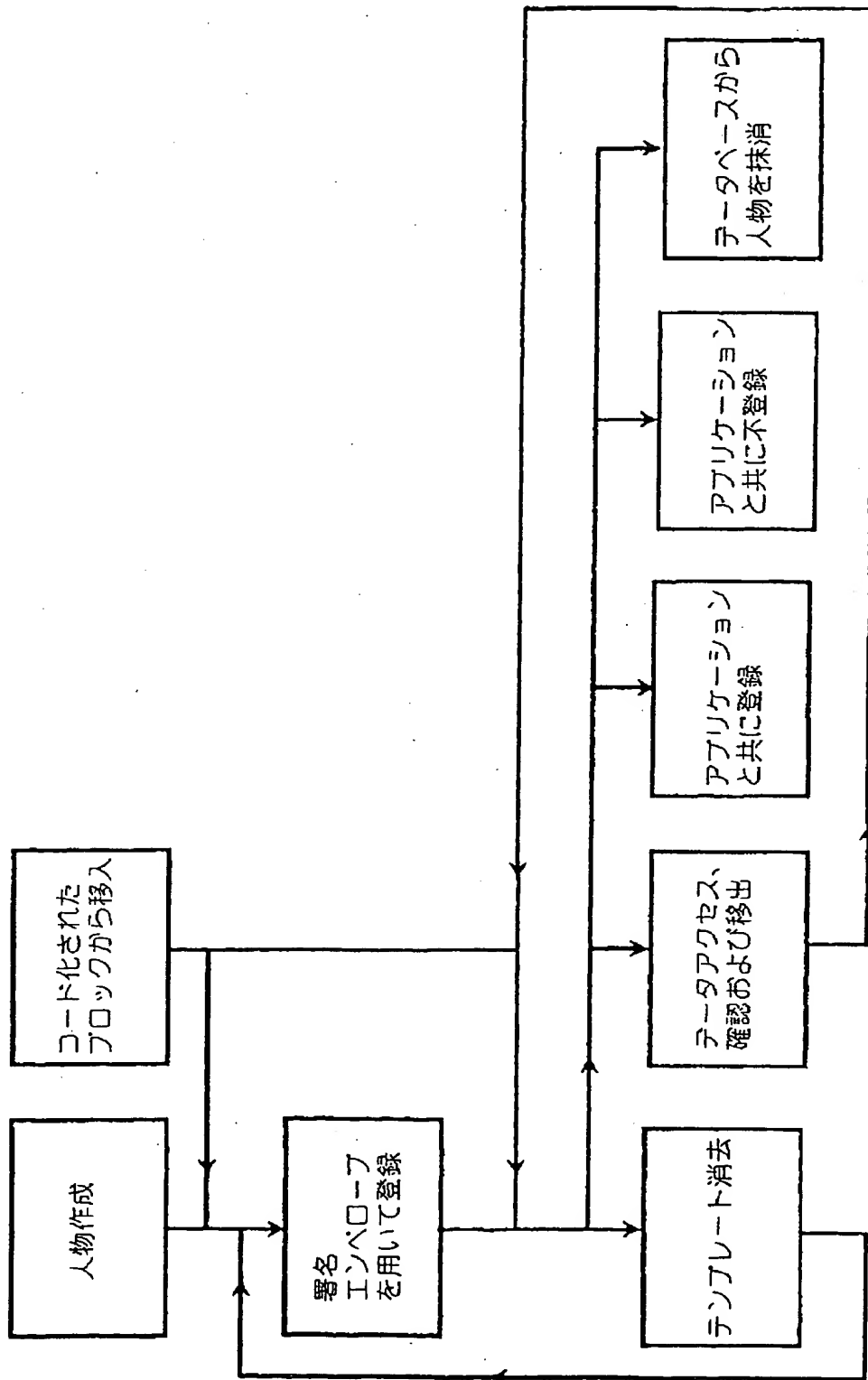


Fig. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11016

A. CLASSIFICATION OF SUBJECT MATTER																				
IPC(6) : Please See Extra Sheet.																				
US CL : Please See Extra Sheet.																				
According to International Patent Classification (IPC) or to both national classification and IPC																				
B. FIELDS SEARCHED																				
Minimum documentation searched (classification system followed by classification symbols)																				
U.S. : Please See Extra Sheet.																				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched																				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)																				
C. DOCUMENTS CONSIDERED TO BE RELEVANT																				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																		
X --- Y	US, A, 5,195,133 (KAPP ET AL.) 16 March 1993, see Figure 5, column 2, lines 22-42, column 3, line 61 through column 4, line 12 and column 5, line 53 through column 6, line 68.	1-2, 7-17, 38-41, 46-52, 57-73 ----- 3-6, 42-45, 53-56																		
X --- Y	US, A, 5,297,202 (KAPP ET AL.) 22 March 1994, see column 5, line 53 through column 7, line 3.	1-2, 7-17, 38-41, 46-52, 57-73 ----- 3-6, 42-45, 53-56																		
Y	US, A, 5,322,978 (PROTHEROE ET AL.) 21 June 1994, see Figure 6.	1-17, 38-73																		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.																				
<table border="0"> <tr> <td>* Special categories of cited documents:</td> <td>* T</td> <td>later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</td> </tr> <tr> <td>* A* document defining the general state of the art which is not considered to be part of particular relevance</td> <td>* X*</td> <td>document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</td> </tr> <tr> <td>* B* earlier document published on or after the international filing date</td> <td>* Y*</td> <td>document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</td> </tr> <tr> <td>* L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</td> <td>* Z*</td> <td>document member of the same patent family</td> </tr> <tr> <td>* O* document referring to an oral disclosure, use, exhibition or other means</td> <td></td> <td></td> </tr> <tr> <td>* P* document published prior to the international filing date but later than the priority date claimed</td> <td></td> <td></td> </tr> </table>			* Special categories of cited documents:	* T	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	* A* document defining the general state of the art which is not considered to be part of particular relevance	* X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	* B* earlier document published on or after the international filing date	* Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	* L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	* Z*	document member of the same patent family	* O* document referring to an oral disclosure, use, exhibition or other means			* P* document published prior to the international filing date but later than the priority date claimed		
* Special categories of cited documents:	* T	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention																		
* A* document defining the general state of the art which is not considered to be part of particular relevance	* X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone																		
* B* earlier document published on or after the international filing date	* Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art																		
* L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	* Z*	document member of the same patent family																		
* O* document referring to an oral disclosure, use, exhibition or other means																				
* P* document published prior to the international filing date but later than the priority date claimed																				
Date of the actual completion of the international search		Date of mailing of the international search report																		
04 OCTOBER 1995		31 OCT 1995																		
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231		Authorized officer <i>Andrew W. Johns</i> ANDREW W. JOHNS																		
Facsimile No. (703) 305-3230		Telephone No. (703) 305-8576																		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11016

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US. A. 4,495,644 (PARKS ET AL.) 22 January 1985, see Table 1 in columns 13-16.	3-6, 42-45, 53-56
A	US, A, 5,091,975 (BERGER ET AL.) 25 February 1992.	1-73
A	US, A, 5,339,361 (SCHWALM ET AL.) 16 August 1994.	1-73
A	Newsbytes News Network, 8 March 1993, "Mobile World-- Signing Documents Remotely By Pen Computer."	1-73
A	Computerworld, 14 June 1993, page 57, "Execs Can Sign Papers By Remote Control; Pen Computing-Based System Allows Addition of Handwritten Notes."	1-73

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11016

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (6):

G06K 9/00

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

382/119, 232

B. FIELDS SEARCHED

Minimum documentation searched

Classification System: U.S.

382/119, 120, 121, 122, 123, 232; 178/18; 340/825.3, 825.33, 825.34; 283/70, 75; 395/155, 161; 380/23

フロントページの続き

(81) 指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, MW, SD, SZ, UG), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN

(72) 発明者 ニューマン, ジェレミー マーク
イギリス国, サマセット ビーエー11 1
イーエル, フロム, シェパーズ バルトン

11

【要約の続き】

評点を得るための署名エンベロープ内に記憶された一揃いの計測値と比較される。本発明は、文書の性質、重大さ及び／又は内容に関して署名者に警告するための重要プロンプト機能を含んでいる。重要プロンプト (22) は同様に署名記録の一部として署名エンベロープの中に記憶することができる。